

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-037750  
(43)Date of publication of application : 10.02.1994

(51)Int.Cl. H04L 9/06  
H04L 9/14  
G09C 1/00  
H04L 12/28

(21)Application number : 04-191893  
(22)Date of filing : 20.07.1992

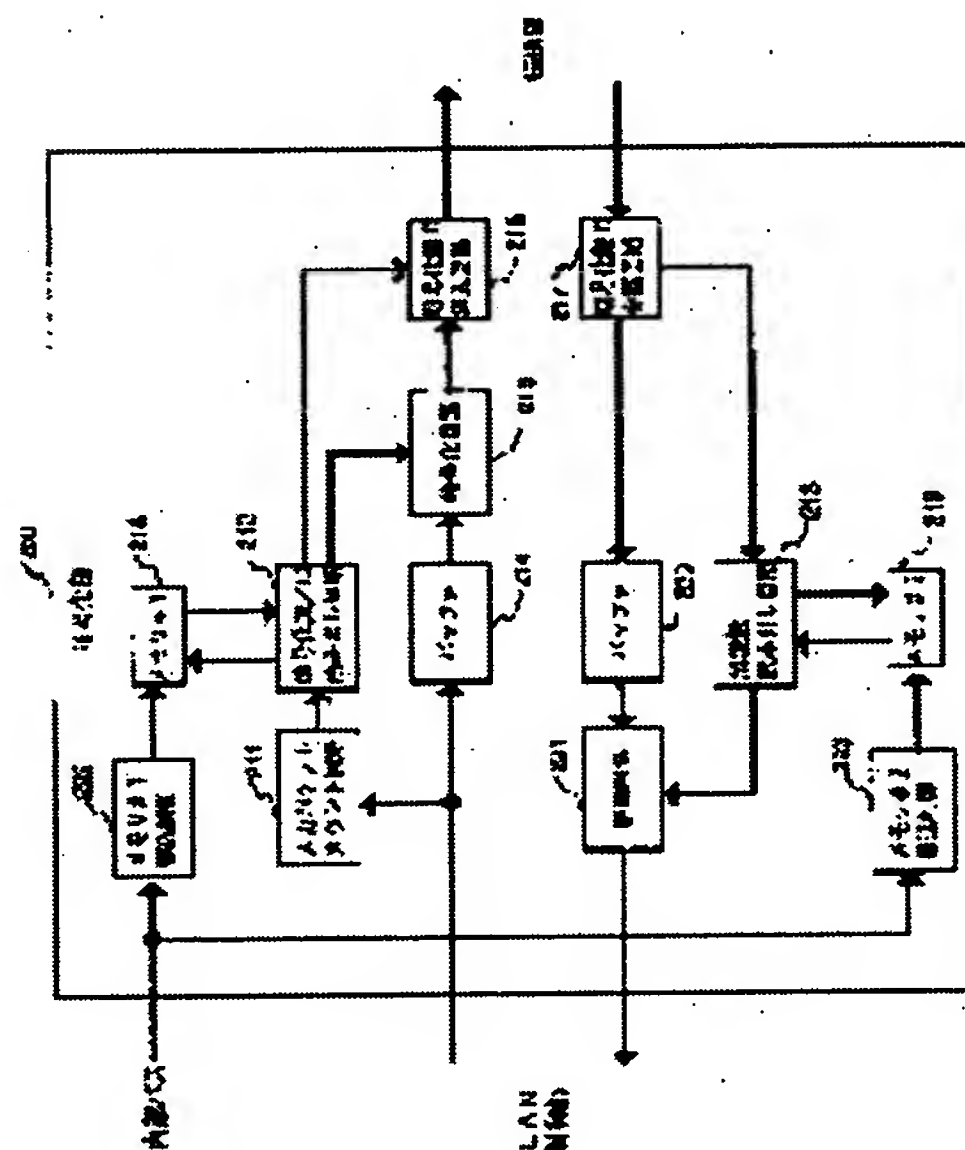
(71)Applicant : HITACHI LTD  
(72)Inventor : ONO MASAFUMI  
TAKIYASU YOSHIHIRO  
ISHIDO TOMOAKI  
SUZUKI HIDEYA

## (54) INFORMATION TRANSFER SYSTEM

### (57)Abstract:

PURPOSE: To decode ciphered information accurately even in ciphering communication using plural ciphering keys by transferring an identification number representing definitely a ciphered key/- decoding key together with ciphered information.

CONSTITUTION: An input packet count circuit 211 in a ciphering section 200 counts number of packets inputted from a LAN control section and transfers a count to a ciphering key/ID read circuit 212. Then the ciphering key/ID read circuit 212 reads a ciphering key identifier definitely representing the ciphering key used for ciphering a packet from a memory 213. That is, a means transferring the ciphering key together with ciphering information informs the ciphering key attended with the ciphering information to a reception terminal equipment. Then a means deciding a decoding key from the ciphering key in the received information in the reception terminal equipment decides a decoding key corresponding to the ciphering key used by the transmission terminal equipment.



## LEGAL STATUS

[Date of request for examination] 09.04.1999  
[Date of sending the examiner's decision of rejection] 22.04.2003  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平6-37750

(43) 公開日 平成6年(1994)2月10日

(51) Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
				9/14
G 0 9 C 1/00		9194-5L		
		7117-5K	H 0 4 L 9/02	Z
		8529-5K	11/00	3 1 0 Z

審査請求 未請求 請求項の数32(全 27 頁) 最終頁に続く

(21) 出願番号 特願平4-191893

(22) 出願日 平成4年(1992)7月20日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 大野 雅史

東京都国分寺市東恋ヶ窪1丁目280番地

株式会社日立製作所中央研究所内

(72) 発明者 滝安 美弘

東京都国分寺市東恋ヶ窪1丁目280番地

株式会社日立製作所中央研究所内

(72) 発明者 石藤 智昭

東京都国分寺市東恋ヶ窪1丁目280番地

株式会社日立製作所中央研究所内

(74) 代理人 弁理士 小川 勝男

最終頁に続く

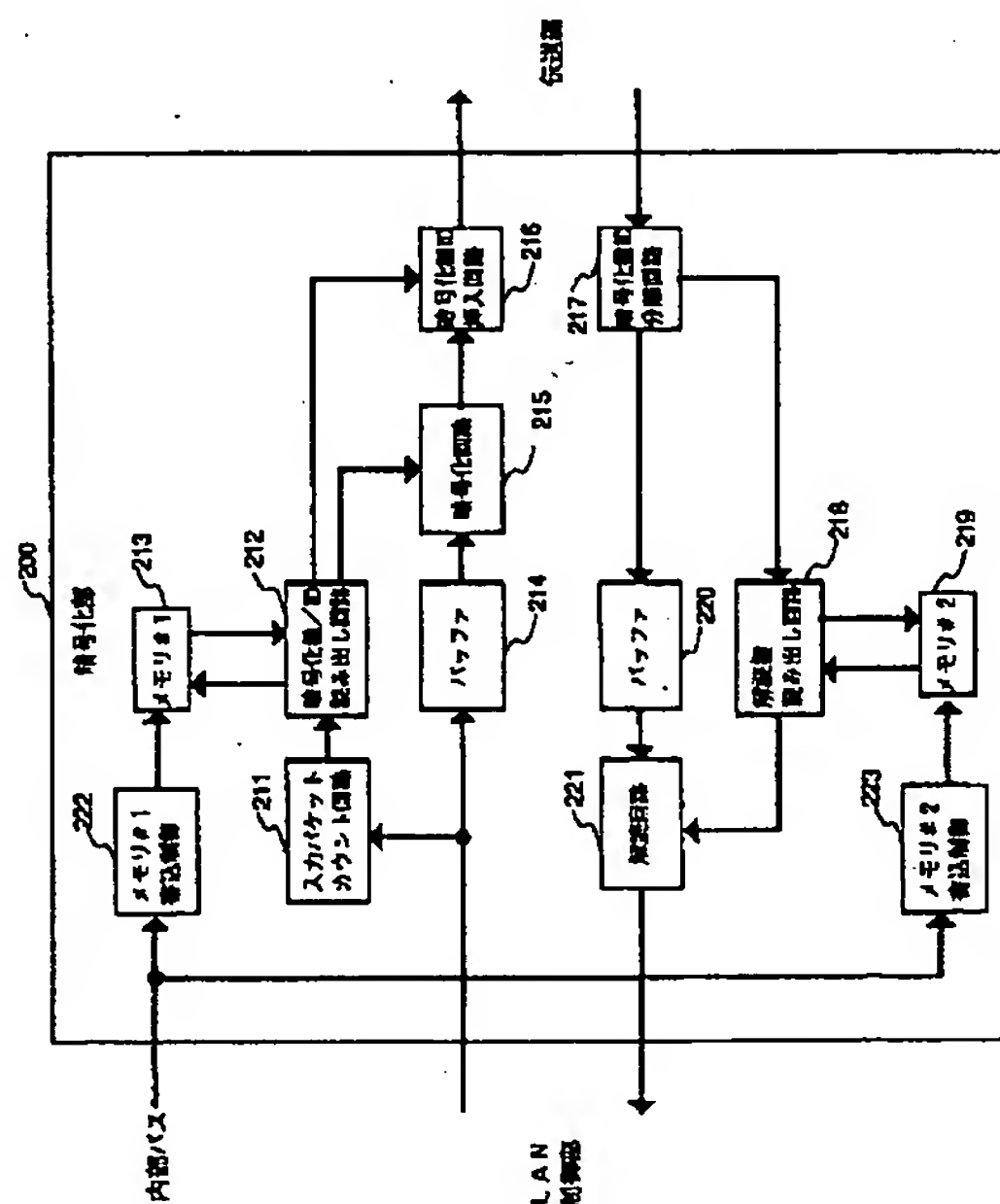
(54) 【発明の名称】 情報転送方式

(57) 【要約】

【構成】 暗号化鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵から解読鍵を決定する手段を受信端末に設ける。

【効果】 暗号化情報と共に暗号化鍵／解読鍵を一意に示す情報を転送するすることで、複数の暗号化鍵を用いる秘匿通信においても受信端末に暗号化鍵／解読鍵の識別情報を随時通知することが可能になるので、暗号化情報を正確に解読することができる。

図1



1

## 【特許請求の範囲】

【請求項1】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は暗号化情報を転送する毎に暗号化鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の暗号化鍵から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項2】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は所定の規則に従って使用する暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗号化鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項3】請求項1または2において、ネットワーク内の全ての通信端末が解読可能な前記暗号化鍵を用いて、少なくとも暗号化鍵を暗号化する情報転送方式。

【請求項4】請求項1または2において、少なくとも暗号化鍵は暗号化せずに転送する情報転送方式。

【請求項5】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は暗号化情報を転送する毎に暗号化鍵に対応する解読鍵を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項6】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は所定の規則に従って使用する暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗号化鍵に対応する解読鍵を暗号化情報と共に転送し、前記受信端末は受信した情報の中の解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項7】請求項5または6において、共通鍵を用いて、少なくとも前記解読鍵を暗号化する情報転送方式。

【請求項8】請求項5または6において、少なくとも前記解読鍵は暗号化せずに転送する情報転送方式。

【請求項9】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する手段を具備し、暗号化情報を転送する毎に前記暗号化鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の暗号化鍵識別子から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項10】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する手段と、所定の規則に従って使用する前記暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記暗

2

号化鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵の識別子から解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項11】請求項9または10において、前記暗号化鍵識別子を決定する手段として、一つあるいは複数の前記暗号化鍵と一つの前記暗号化鍵識別子を関連付けて記憶する手段を具備する情報転送方式。

【請求項12】請求項9、10または11において、前記共通鍵を用いて、少なくとも前記暗号化鍵識別子を暗号化する情報転送方式。

【請求項13】請求項9、10または11において、少なくとも前記暗号化鍵識別子は暗号化せずに転送する情報転送方式。

【請求項14】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段を具備し、暗号化情報を転送する毎に前記解読鍵識別子を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記解読鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項15】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段と、所定の規則に従って使用する前記暗号化鍵を変更する手段を具備し、前記暗号化鍵を変更する毎に前記解読鍵識別子を暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記解読鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読することを特徴とする情報転送方式。

【請求項16】請求項14または15において、前記解読鍵識別子を決定する手段として、一つあるいは複数の前記暗号化鍵と一つの前記解読鍵識別子を関連付けて記憶する手段を具備する情報転送方式。

【請求項17】請求項14、15または16において、前記共通鍵を用いて、少なくとも前記解読鍵識別子を暗号化する情報転送方式。

【請求項18】請求項14、15または16において、少なくとも前記解読鍵識別子は暗号化せずに転送する情報転送方式。

【請求項19】送信端末から受信端末に情報を暗号化し、暗号化情報をバケット化して転送する情報転送方式において、前記送信端末は2種類以上の暗号化鍵を用いて情報を暗号化し、バケットを組み立て、前記受信端末に転送することを特徴とする情報転送方式。

【請求項20】請求項19において、前記送信端末は使用する前記暗号化鍵を一意に示す前記暗号化鍵識別子を



3

決定する手段を具備し、前記暗号化情報を転送する毎に前記暗号化鍵識別子を前記暗号化情報と共に転送し、前記受信端末は受信した情報の中の前記暗号化鍵識別子から前記解読鍵を決定する手段を具備し、前記解読鍵を用いて前記受信情報を解読する情報転送方式。

【請求項21】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定し、前記受信端末は受信した情報の中の前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定することを特徴とする情報転送方式。

【請求項22】請求項21において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、解読鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項23】請求項21において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記受信端末アドレスと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、前記解読鍵を決定する手段として、一つあるいは複数の前記受信端末アドレスと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項24】請求項21において、前記暗号化鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと前記受信端末アドレスの組み合わせと一つの前記暗号化鍵を関連付けて記憶する手段を具備し、前記解読鍵を決定する手段として、一つあるいは複数の前記送信端末アドレスと前記受信端末アドレスの組み合わせと一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項25】請求項21、22、23または24において、前記送信端末は、少なくとも前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方を暗号化せずに、前記転送情報と共に転送する情報転送方式。

【請求項26】請求項21、22、23または24において、前記送信端末は、前記送信端末アドレスと前記受信端末アドレスのいずれか一方、あるいは両方を共通鍵を用いて暗号化して、前記転送情報と共に転送する情報転送方式。

【請求項27】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、前記送信端末は、前記送信端末から前記受信端末への転送経路を示すルート情報から暗号化鍵を決定し、前記受信端末は受信した情報の中の前記ルート情報から解読鍵を決定することを特徴とする情報転送方式。

【請求項28】請求項27において、前記暗号化鍵を決定する手段として、一つあるいは複数のルート情報と一

4

つの前記暗号化鍵を関連付けて記憶する手段を具備し、解読鍵を決定する手段として、一つあるいは複数の前記ルート情報と一つの前記解読鍵を関連付けて記憶する手段を具備する情報転送方式。

【請求項29】請求項27または28において、前記送信端末は少なくとも前記ルート情報を暗号化せずに前記転送情報と共に転送する情報転送方式。

【請求項30】請求項27または28において、前記送信端末は少なくとも前記ルート情報を前記共通鍵を用いて暗号化して前記転送情報と共に転送する情報転送方式。

【請求項31】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、フロッピーディスクからのローディング、リード・オンリー・メモリからのローディング、通信端末あるいは制御端末からのコマンド入力の内、少なくとも一つの手段により暗号化鍵を設定することを特徴とする情報伝送方式。

【請求項32】送信端末から受信端末に情報を暗号化して転送する情報転送方式において、フロッピーディスクからのローディング、リードオンリーメモリからのローディング、通信端末あるいは制御端末からのコマンド入力の内、任意の複数の設定手段を有し、更に任意の設定手段を選択することを特徴とする情報転送方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、送信側通信端末（以下、送信端末と称す）から受信側通信端末（以下、受信端末と称す）に情報を暗号化して転送する情報転送方式に係り、特に、転送情報の送信先によって異なる暗号化アルゴリズム（以下、暗号化鍵と称す）を用いて情報を暗号化し転送する情報転送方式に関する。

【0002】

【従来の技術】暗号を用いた従来の秘匿通信方式として、特開平3-26227号公報に開示の技術がある。

【0003】上記従来技術では、二つの通信局間で秘匿通信を行うために、双方の通信局に多数の暗証コードおよび暗号コード（暗号化鍵）を同じアドレスに記憶した暗証／暗号メモリを具備する。送信局は受信局に対して暗証／暗号メモリのアドレスを指定した応答要求信号を送信し、受信局は指定されたアドレスに記憶された暗証コードを読み出して、暗証コードを応答信号にのせて送信局に返信する。送信局は応答信号の暗証コードが正しいことを確認した後に、同アドレスの暗号コードを読み出し、暗号コードを用いて情報を暗号化した後に受信局に送信する。一方、受信局はアドレスの暗号コードを読み出し、暗号コードを用いて受信情報の解読を行う。

【0004】

【発明が解決しようとする課題】上記従来技術をローカルエリアネットワーク（以下、LANと称す）の様なコネクションレス通信（以下、CL通信と称す）に適用す

る場合には次のような問題点が生じる。

【0005】 先ず、CL通信には明確な通信の開始が無いので、秘匿通信に先立って暗号コードを転送することが出来ないという問題点がある。これに対して単一の暗号コードを使用するという方式が考えられるが、単一暗号コードを使用した場合は暗号コードを第三者が獲得しネットワーク内の情報を無断で入手する危険性が高くなるので好ましくない。

【0006】 ネットワークのセキュリティを向上させるには複数の暗号コードを用いれば良いが、CL通信では前述の様に通信に先立って暗号コードを通知することが出来ないで、次のような新たな問題点が発生する。すなわち、CL通信ではネットワーク内の各端末が受信するのは必ずしも自分宛の情報とは限らない。即ち、各端末はネットワーク上の転送情報を監視し、転送情報（パケット）に含まれるルート情報に基づきパケットが自分宛か否かを判断しパケットの取捨選択を行う。ここで、ネットワーク内で複数の異なる暗号化コードを用いて複数の異なるルート情報を暗号化した場合、異なるルート情報から同一の暗号化ルート情報が生成することが考えられる。即ち、このような場合には送受信端末間で暗号コードを一致させておかないと、本来受信しない情報を誤って受信してしまうことになる。

【0007】 従来技術の類似技術として、CL通信の任意の時点（例えば、始業時間）に暗号コードを通知するようにして、更に、異なるルート情報からは異なる暗号化ルート情報しか生成しないようにしても次のような問題点が生じる。すなわち、前述の様に、CL通信ではネットワーク上のパケットの取捨選択によりパケットを受信するか否かを決定するので、受信端末はパケット受信毎に全ての暗号コードを用いてパケットを解読しなくてはならない。これはネットワークのスループットの低下の原因になるばかりでなく、ハード量の増加の原因にもなる。

【0008】 本発明の目的は、送受信端末間の情報授受の機密性を維持するために複数の暗号化コード（暗号化鍵）を用いる情報転送方式において、暗号化情報の誤受信とこれに伴うスループットの低下、およびハード量の増加を防ぐ情報転送方式を提供することにある。

【0009】

【課題を解決するための手段】 前記課題を解決する第一の手段として、暗号化鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵から解読鍵を決定する手段を受信端末に設ける。

【0010】 前記課題を解決する第二の手段として、暗号化鍵に対応する解読鍵を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の解読鍵を読み出す手段を受信端末に設ける。

【0011】 前記課題を解決する第三の手段として、使用する暗号化鍵を一意に示す暗号化鍵識別子を決定する

手段と、前記暗号化鍵識別子を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の暗号化鍵識別子から解読鍵を決定する手段を受信端末に設ける。

【0012】 前記課題を解決する第四の手段として、使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を決定する手段と、前記解読鍵識別子を暗号化情報と共に転送する手段を送信端末に設け、受信した情報の中の解読鍵識別子から解読鍵を決定する手段を受信端末に設ける。

10 【0013】 前記課題を解決する第五の手段として、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定する手段を送信端末に設け、受信した情報の中の送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定する手段を受信端末に設ける。

【0014】 前記課題を解決する第六の手段として、ルート情報から暗号化鍵を決定する手段を送信端末に設け、受信した情報の中のルート情報から解読鍵を決定する手段を受信端末に設ける。

20 【0015】

【作用】 第一の解決手段を用いた情報転送方式では、暗号化鍵を暗号化情報と共に転送する手段により、暗号化情報に付随して受信端末に暗号化鍵を通知することが可能になる。更に、受信した情報の中の暗号化鍵から解読鍵を決定する手段により、受信端末は送信端末が使用した暗号化鍵に対応する解読鍵を決定することが出来る。本情報転送方式では暗号化情報と暗号化鍵が対になって転送され、更に暗号化鍵から解読鍵を決定することが出来るので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

30 【0016】 第二の解決手段を用いた情報転送方式では、暗号化鍵に対応する解読鍵を暗号化情報と共に転送する手段により、暗号化情報に付随して受信端末に解読鍵を通知することが可能になる。更に、受信した情報の中の解読鍵を読み出す手段により、受信端末は送信端末が使用した暗号化鍵に対応する解読鍵を決定することが出来る。本情報転送方式では暗号化情報と対応する解読鍵が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

40 【0017】 第三の解決手段を用いた情報転送方式では、使用する暗号化鍵を一意に示す暗号化鍵識別子を暗号化情報と共に転送する手段により、受信端末に暗号化鍵識別子を通知することが可能になる。更に、暗号化鍵識別子から解読鍵を決定する手段により、暗号化鍵識別子に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では暗号化情報と暗号化鍵識別子が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

50 【0018】 第四の解決手段を用いた情報転送方式で



は、使用する暗号化鍵に対応する解読鍵を一意に示す解読鍵識別子を暗号化情報と共に転送する手段により、受信端末に解読鍵識別子を通知することが可能になる。更に、解読鍵識別子から解読鍵を決定する手段により、解読鍵識別子に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では暗号化情報と解読鍵識別子が対になって転送されるので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが可能になる。

【0019】第五の解決手段を用いた情報転送方式では、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から暗号化鍵を決定する手段と、受信した情報の中の送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方から解読鍵を決定する手段により、送信端末アドレスと受信端末アドレスのいずれか一方、あるいは両方のアドレスに対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式では送信端末アドレスと受信端末アドレスを暗号化情報と共に転送するので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが出来る。

【0020】第六の解決手段を用いた情報転送方式では、ルート情報から暗号化鍵を決定する手段と、受信した情報の中のルート情報から解読鍵を決定する手段により、ルート情報に対して一組の暗号化鍵／解読鍵が定まる。本情報転送方式ではルート情報を暗号化情報と共に転送するので、複数の暗号化鍵を用いる場合でも暗号化情報を正確に解読することが出来る。

【0021】

【実施例】図2は本発明を用いたLAN接続ボード140（以下、LANインタフェースと称す）を装着したワークステーション（以下、WSと称す）本体100のブロック図である。

【0022】図2において、ユーザI/Oインタフェース110、CPU120、メモリ130、LANインタフェース140、FD制御部150が内部バス160で接続されている。ユーザI/Oインタフェース110はWS本体100と入力装置（キーボード）および出力装置（ディスプレイ）のインタフェースであり、キーボードからの入力信号の内部バス160への転送、内部バス160からの信号のディスプレイへの出力等の機能を持つ。尚、本実施例では入力装置をキーボード、出力装置をディスプレイとしたが本構成は本発明を限定するものではない。

【0023】CPU120はキーボードから入力する情報、およびLANインタフェース140を介して入力する他端末等からの情報の処理と各機能ブロックの制御を行うブロックである。メモリ130は前述の各種情報を格納する機能ブロックであり、CPU120の処理待ち、ディスプレイへの出力待ち等の場合に当該情報を格納する。LANインタフェース140はWSをネットワーク（LAN）に接続するための機能を有するブロック

であり、内部バス160の伝送フォーマットとLANの伝送フォーマットの変換を行うと共に、MAC(Media Access Control)層の終端、転送情報の暗号化を行う。FD制御部150はCPU120の指示に従って、フロッピーディスク（以下FD）からのローディング、FDへのセーブ等の機能を持つ。内部バス160はWSが処理するデータを転送するデータバスと、各機能ブロックを制御するための制御情報を転送する制御情報バスからなる。

10 【0024】図3はLANインタフェース140の機能ブロック図である。LANインタフェース140はバスインタフェース170、LAN制御部180、ROM190、暗号化部200、伝送部210から構成される。

【0025】バスインタフェース170は内部バス160からの情報ブロックの切り出し、情報ブロックのLAN制御部180への転送、更に、LAN制御部180から転送された情報ブロックのバッファリング、情報ブロックの内部バスへの乗せ換えを行う。LAN制御部180はパケットの生成／分解、パケットヘッダの付加／削除等のMACレイヤ機能を実現するブロックである。パケットヘッダには送信端末アドレス（送信元アドレス）と受信端末アドレス（宛先アドレス）が含まれる。送信元アドレスにはROM190に登録されているMACアドレスが書き込まれる。ROM190に登録されているMACアドレスは、WSだけに割り当てられたアドレスである。一方、宛先アドレスにはパケットの送信先のWSに割り当てられたMACアドレスが書き込まれる。これらの宛先WSのMACアドレスはデータベースとしてLAN制御部180内のメモリに記憶されている。暗号化部200はLAN制御部180からの情報の暗号化を行うと共に、LANから受信した暗号化情報を解読しLAN制御部180に転送する。伝送部210は暗号化部200からの情報を、接続するLANの伝送フォーマットに変換しLANに転送する。また、LANから転送される情報を自WS内のフォーマットに変換する。

【0026】次に図1を用いて暗号化部200を詳細に説明する。図1において、入力パケットカウント回路211はLAN制御部180から入力するパケット数をカウントし、カウント値を暗号化鍵／ID読み出し回路212に転送する。暗号化鍵／ID読み出し回路212はカウント値に基づき、パケットの暗号化に使用する暗号化鍵と暗号化鍵を一意に示す暗号化鍵識別子（以下、暗号化鍵IDと称す）をメモリ213より読み出す。

【0027】図4(a)にメモリ213の構成例を示す。本実施例では0から255までのカウント値301に対して、一対一に対応するように暗号化鍵302が256種類登録されており、各暗号化鍵に16進表示で00からFFまでの暗号化鍵ID303が登録されている。尚、異なる複数の暗号化鍵IDに対して同一の暗号化鍵を対応させることも可能である。そのような場合に

は、256種類のカウンタ値と暗号化鍵IDに対して256種類以下の暗号化鍵が登録される。更に、暗号化鍵／ID読み出し回路212は暗号化鍵を暗号化回路215に転送すると共に、暗号化鍵IDを暗号化鍵ID挿入回路216に転送する。バッファ214は暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。暗号化鍵ID挿入回路216はパケットの所定の位置に、暗号化鍵／ID読み出し回路212より転送された暗号化鍵IDを挿入する。

【0028】図5に本実施例における暗号化鍵ID504の挿入位置を示す。パケット500はパケットヘッダと情報領域501から構成される。パケットヘッダ内には宛先アドレス502と送信元アドレス503が書き込まれている。暗号化鍵ID504はユーザ情報505とパケットヘッダの間に挿入する。MAC層では、暗号化鍵ID504とユーザ情報505を情報領域501として扱うので、暗号化鍵ID504の挿入はMAC層プロトコルには影響を及ぼさない。

【0029】一方、暗号化回路215はバッファ214より入力するパケットを暗号化し、暗号化鍵ID挿入回路216に転送する。本実施例では、暗号化鍵IDはネットワーク内の全ての通信機器が解読可能な暗号化鍵（以下、共通暗号化鍵と称す）を用いて暗号化し、その他の部分はメモリ213より読み出した個別の暗号化鍵を用いて暗号化する。

【0030】次に、LANから暗号化情報を受信したときの処理について説明する。暗号化鍵ID分離回路217は受信暗号化パケットから暗号化鍵IDの区間を切り出し、解読鍵読み出し回路218に転送する。暗号化鍵ID以外の部分はそのままバッファ220に格納される。解読鍵読み出し回路218は暗号化鍵IDに基づき、メモリ219より解読鍵を読み出す。暗号化鍵IDは共通暗号化鍵で暗号化されているので、全ての受信端末は暗号化鍵IDを解読することができる。尚、本実施例では暗号化鍵IDの暗号化に共通暗号化鍵を用いているので平文の暗号化鍵IDと暗号化した暗号化鍵IDは一対一に対応するので、受信したパケットの暗号化鍵IDを解読せずに用いて解読鍵を選択することも可能である。また、暗号化鍵IDを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合は暗号化鍵ID分離回路217が切り出した暗号化鍵IDをそのまま用いて解読鍵を選択する。

【0031】図4(b)にメモリ219の構成例を示す。本実施例では16進表示で00からFFまでの暗号化鍵ID401に対して、一対一に対応するように解読鍵402が256種類登録されている。尚、メモリ213と同様に異なる複数の暗号化鍵IDに対して同一の解読鍵を対応させることも可能である。そのような場合には256種類の暗号化鍵IDに対して256種類以下の解読鍵が登録される。解読鍵読み出し回路218は暗号化

鍵IDで一意に定まる解読鍵を読み出し、解読回路221に転送する。解読回路221は、バッファ220より入力するパケットを解読鍵を用いて解読し、LAN制御部180に転送する。

【0032】次に本実施例におけるカウンタ値／暗号化鍵／暗号化鍵ID／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(FD)より設定データをロードする。カウンタ値／暗号化鍵／暗号化鍵IDを登録するメモリ213への設定データの書き込み制御はメモリ書込制御222が行う。一方、暗号化鍵ID／解読鍵を登録するメモリ219への設定データの書き込み制御はメモリ書込制御223が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ書込制御222およびメモリ書込制御223に転送される。書込制御222および223はCPU120の指示に基づき、メモリ213およびメモリ219の登録内容の書き換えを行う。

【0033】次に図6、図7を用いて第二の実施例について説明する。本実施例ではLAN制御部180から入力するパケットの宛先アドレスに基づいて使用する暗号化鍵を決定する。尚、本実施例は第一の実施例と暗号化部200の動作のみが異なるので、暗号化部200のみ説明する。

【0034】図6において、宛先アドレス読み出し回路224はLAN制御部180から入力するパケットの宛先アドレスを読み出し、暗号化鍵読み出し回路225に転送する。暗号化鍵読み出し回路225は宛先アドレスに基づき、使用する暗号化鍵をメモリ213より読み出す。

【0035】図7(a)に本実施例におけるメモリ213の構成例を示す。メモリ213では256種類の送信パケット宛先アドレス304(DA#0~DA#255)に対して、一対一に対応するように暗号化鍵302が256種類登録されている。宛先アドレスには各端末への個別通信用のアドレスと複数の端末に共通に付与されているグループ通信用のアドレスと、全ての端末に共通に付与されている一斉通報通信用のアドレスがある。尚、異なる複数の宛先アドレスに対して同一の暗号化鍵を対応させることも可能である。そのような場合には256種類の宛先アドレスに対して256種類以下の暗号化鍵が登録される。更に、宛先アドレスと送信元アドレスの組み合わせに対して、一対一に対応するように暗号化鍵を登録することも可能である。更に、暗号化鍵読み出し回路225は暗号化鍵を暗号化回路215に転送する。バッファ214は暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。暗



号化回路215はバッファ214より入力するパケットを暗号化し、伝送部210に転送する。本実施例では、宛先アドレスと送信元アドレスは共通暗号化鍵を用いて暗号化し、その他の部分はメモリ213より読み出した暗号化鍵を用いて暗号化する。

【0036】本実施例では、第一の実施例における暗号化鍵IDのような特有のパラメータを使用しないので、暗号化部200と伝送部210の間で授受するパケットフォーマットはLAN制御部がサポートするMAC層プロトコルのパケットフォーマットと一致する。

【0037】次に、LANから暗号化情報（パケット）を受信したときの処理について説明する。宛先アドレス分離回路226は暗号化パケットから宛先アドレスの区間を複写し、解読鍵読み出し回路218に転送する。解読鍵読み出し回路218は宛先アドレスに基づき、メモリ219より解読鍵を読み出す。宛先アドレスは共通暗号化鍵で暗号化されているので、全ての受信端末は宛先アドレスを解読することができる。尚、本実施例では宛先アドレスの暗号化に共通暗号化鍵を用いていることから平文の宛先アドレスと暗号化した宛先アドレスは一対一に対応するので、受信したパケットの宛先アドレスを解読せずに用いて解読鍵を選択することも可能である。また、宛先アドレスを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合は宛先アドレス分離回路226が複写した宛先アドレスをそのまま用いて解読鍵を選択する。

【0038】図7(b)にメモリ219の構成例を示す。本実施例では(N+2)種類の受信パケットの宛先アドレス403に対して(N+2)種類の解読鍵402が一対一に対応するように登録されている。具体的には、自WSが個別通信の受信端末となる場合の自アドレス1種類、自WSを含むグループに対するグループ通信を行う場合のグループアドレスN種類、全ての端末に対する同報通信を行う場合の一斉同報アドレス1種類の計(N+2)種類のアドレスに対して、一対一に対応するように(N+2)種類の解読鍵402が登録されている。尚、異なる複数の受信パケット宛先アドレスに対して同一の解読鍵を対応させることも可能である。そのような場合には(N+2)種類の宛先アドレスに対して(N+2)種類以下の解読鍵が登録される。更には、宛先アドレスと発信元アドレスの組み合わせに対して、一対一に対応するように解読鍵を登録することも可能である。解読鍵読み出し回路218は宛先アドレスで一意に定まる解読鍵を読み出し、解読回路221に転送する。解読回路221はバッファ220より入力するパケットを解読鍵を用いて解読し、LAN制御部180に転送する。

【0039】次に本実施例における送信パケット宛先アドレス/暗号化鍵および受信パケット宛先アドレス/解読鍵の設定方法について説明する。本実施例ではシステ

ム構築時に、FDより設定データをロードする。送信パケット宛先アドレス/暗号化鍵を登録するメモリ213への設定データの書き込み制御はメモリ書込制御222が行う。一方、受信パケット宛先アドレス/解読鍵を登録するメモリ219への設定データの書き込み制御はメモリ#2書込制御223が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ書込制御222およびメモリ書込制御223に転送される。書込制御222、223はCPU120の指示に従い、メモリ213、メモリ219の登録内容の書き換えを行う。

【0040】次に図8、図9を用いて第三の実施例について説明する。本実施例ではLAN制御部180から入力するパケットのルート情報に基づいて使用する暗号化鍵を決定する。尚、本実施例も前述の第一の実施例と暗号化部200の動作のみが異なるので、暗号化部200のみ説明する。

【0041】図8において、ルート情報読み出し回路227はLAN制御部180から入力するパケットのルート情報を読み出し、暗号化鍵読み出し回路225に転送する。暗号化鍵読み出し回路225はルート情報に基づき、使用する暗号化鍵をメモリ213より読み出す。

【0042】図9(a)に本実施例におけるメモリ213の構成例を示す。メモリ213では256種類の送信パケットルート情報305(VCN#0~VCN#255)に対して、一対一に対応するように暗号化鍵302が256種類登録されている。尚、ルート情報の設定方法は任意であり本発明を制限するものではない。暗号化鍵読み出し回路225は暗号化鍵を暗号化回路215に転送する。バッファ214は前記暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。暗号化回路215はバッファ214より入力するパケットを暗号化し、伝送部210に転送する。本実施例では、ルート情報は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ213より読み出した暗号化鍵を用いて暗号化する。

【0043】本実施例でも第一の実施例における暗号化鍵IDのような特有のパラメータを使用しないので、暗号化部200と伝送部210の間で授受するパケットフォーマットはLAN制御部がサポートするMAC層プロトコルのパケットフォーマットと完全に一致する。

【0044】次に、LANから暗号化情報（パケット）を受信したときの処理について説明する。ルート情報分離回路228は暗号化パケットからルート情報の区間を複写し、解読鍵読み出し回路218に転送する。解読鍵読み出し回路218はルート情報に基づき、メモリ219より解読鍵を読み出す。ルート情報は共通暗号化鍵で



暗号化されているので、全ての受信端末はルート情報を解読することができる。尚、本実施例ではルート情報の暗号化に共通暗号化鍵を用いているので平文のルート情報と暗号化したルート情報は一対一に対応するので、受信したパケットのルート情報を解読せずに用いて解読鍵を選択することも可能である。また、ルート情報を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合にはルート情報分離回路228が複写したルート情報をそのまま用いて解読鍵を選択する。

【0045】図9(b)にメモリ219の構成例を示す。本実施例では受信パケットのルート情報404に対して、一対一に対応するように256種類の解読鍵402が登録されている。尚、異なる複数のルート情報に対して同一の解読鍵を対応させることも可能である。そのような場合には256種類のルート情報に対して256種類以下の解読鍵が登録される。解読鍵読み出し回路218はルート情報で一意に定まる解読鍵を読み出し、解読回路221に転送する。解読回路221はバッファ220より入力するパケットを解読鍵を用いて解読し、LAN制御部180に転送する。

【0046】次に本実施例における送信パケットルート情報/暗号化鍵および受信パケットルート情報/解読鍵の設定方法について説明する。本実施例ではシステム構築時に、FDより設定データをロードする。送信パケットルート情報/暗号化鍵を登録するメモリ213への設定データの書き込み制御はメモリ213の書込制御222が行う。一方、受信パケットルート情報/解読鍵を登録するメモリ219への設定データの書き込み制御はメモリ219の書込制御223が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ#1書込制御222およびメモリ#2書込制御223に転送される。書込制御222および223はCPU120の指示に基づき、メモリ213およびメモリ219の登録内容の書き換えを行う。

【0047】次に図10、図11を用いて第四の実施例について説明する。本実施例ではパケットを送信する通信端末のMACアドレスに基づいて使用する暗号化鍵を決定する。従って、物理的に一つの通信端末が複数のMACアドレスを有する場合には一端が複数の暗号化鍵を有することになり、複数の通信端末が一つのMACアドレスを共有する場合には複数の端末が一つの暗号化鍵を共有することになる。尚、本実施例も前述の第一の実施例と暗号化部200の動作のみが異なるので、暗号化部200のみ説明する。

【0048】図10において、送信元アドレス読み出し回路229はLAN制御部180から入力するパケットの送信元アドレスを読み出し、暗号化鍵読み出し回路2

25に転送する。暗号化鍵読み出し回路225は前記送信元アドレスに基づき、使用する暗号化鍵をメモリ213より読み出す。

【0049】図11(a)に本実施例におけるメモリ213の構成例を示す。本実施例では1種類の送信パケット送信元アドレス306に対して1種類の暗号化鍵302が登録されている。暗号化鍵読み出し回路225は暗号化鍵を暗号化回路215に転送する。バッファ214は暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。暗号化回路215はバッファ214より入力するパケットを暗号化し、伝送部210に転送する。本実施例では、宛先アドレスと送信元アドレスは共通暗号化鍵を用いて暗号化し、その他の部分はメモリ213より読み出した暗号化鍵を用いて暗号化する。

【0050】本実施例でも第一の実施例における暗号化鍵IDのような特有のパラメータを使用しないので、暗号化部200と伝送部210の間で授受するパケットフォーマットはLAN制御部がサポートするMAC層プロトコルのパケットフォーマットと一致する。

【0051】次に、LANから暗号化情報(パケット)を受信したときの処理について説明する。送信元アドレス分離回路230は暗号化パケットから送信元アドレスの区間を複写し、解読鍵読み出し回路218に転送する。解読鍵読み出し回路218は送信元アドレスに基づき、メモリ219より解読鍵を読み出す。送信元アドレスは共通暗号化鍵で暗号化されているので、全ての受信端末は送信元アドレスを解読することができる。尚、本実施例では送信元アドレスの暗号化に共通暗号化鍵を用いていることから平文の送信元アドレスと暗号化した送信元アドレスは一対一に対応するので、受信したパケットの送信元アドレスを解読せずに用いて解読鍵を選択することも可能である。また、送信元アドレスを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には送信元アドレス分離回路230が複写した送信元アドレスをそのまま用いて解読鍵を選択する。

【0052】図11(b)にメモリ219の構成例を示す。本実施例では256種類の受信パケットの送信元アドレス405に対して256種類の解読鍵402が一対一に対応するように登録されている。尚、異なる複数の受信パケット送信元アドレスに対して同一の解読鍵を対応させることも可能である。そのような場合には256種類の宛先アドレスに対して256種類以下の解読鍵が登録される。解読鍵読み出し回路218は送信元アドレスで一意に定まる解読鍵を読み出し、解読回路221に転送する。解読回路221はバッファ220より入力するパケットを解読鍵を用いて解読し、LAN制御部180に転送する。

【0053】次に本実施例における送信パケット送信元

アドレス／暗号化鍵および受信パケット送信元アドレス／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、FDより設定データをロードする。送信パケット送信元アドレス／暗号化鍵を登録するメモリ213への設定データの書き込み制御はメモリ213書込制御222が行う。一方、受信パケット送信元アドレス／解読鍵を登録するメモリ219への設定データの書き込み制御はメモリ219の書込制御223が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ213の書込制御222およびメモリ219の書込制御223に転送される。書込制御222および223はCPU120の指示に基づき、メモリ213およびメモリ219の登録内容の書き換えを行う。

【0054】次に図12、図13および14を用いて第五の実施例について説明する。第一の実施例が暗号化鍵IDを暗号化情報と共に転送するのに対して、本実施例は暗号化鍵を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部200の動作のみが異なるので、暗号化部200のみ説明する。

【0055】図12において、入力パケットカウント回路211はLAN制御部180から入力するパケット数をカウントし、カウント値を暗号化鍵読み出し回路231に転送する。暗号化鍵読み出し回路231はカウント値に基づき、パケットの暗号化に使用する暗号化鍵をメモリ213より読み出す。

【0056】図13(a)にメモリ213の構成例を示す。本実施例では0から255までのカウント値301に対して、一対一に対応するように暗号化鍵302が256種類登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵を対応させることも可能である。そのような場合には256種類のカウント値に対して256種類以下の暗号化鍵が登録される。更に、暗号化鍵読み出し回路231は暗号化鍵を暗号化回路215と暗号化鍵挿入回路232に転送する。バッファ214は暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。暗号化鍵挿入回路232はパケットの所定の位置に、暗号化鍵読み出し回路231より転送された暗号化鍵を挿入する。

【0057】図14に本実施例における暗号化鍵506の挿入位置を示す。パケット500はパケットヘッダと情報領域501から構成される。パケットヘッダ内には宛先アドレス502と送信元アドレス503が書き込まれている。暗号化鍵506はユーザ情報505とパケットヘッダの間に挿入する。MAC層では、暗号化鍵506とユーザ情報505を情報領域501として扱うので、暗号化鍵506の挿入はMAC層プロトコルには影

響を及ぼさない。

【0058】一方、暗号化回路215はバッファ214より入力するパケットを暗号化し、暗号化鍵挿入回路232に転送する。本実施例では、暗号化鍵はネットワーク内の全ての通信機器が解読可能な暗号化鍵（以下、共通暗号化鍵と称す）を用いて暗号化し、その他の部分はメモリ213より読み出した個別の暗号化鍵を用いて暗号化する。

【0059】次に、LANから暗号化情報を受信したときの処理について説明する。暗号化鍵分離回路233は受信暗号化パケットから暗号化鍵の区間を切り出し、解読鍵読み出し回路218に転送する。暗号化鍵以外の部分はそのままバッファ220に格納される。解読鍵読み出し回路218は暗号化鍵に基づき、メモリ219より解読鍵を読み出す。暗号化鍵は共通暗号化鍵で暗号化されているので、全ての受信端末は暗号化鍵を解読することができる。尚、本実施例では暗号化鍵の暗号化に共通暗号化鍵を用いていることから平文の暗号化鍵と暗号化した暗号化鍵は一対一に対応するので、受信したパケットの暗号化鍵を解読せずに用いて解読鍵を選択することも可能である。また、暗号化鍵を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には暗号化鍵分離回路233が切り出した暗号化鍵をそのまま用いて解読鍵の選択を行う。

【0060】図13(b)にメモリ219の構成例を示す。本実施例では256種類の暗号化鍵406(C-Key#0~C-Key#255)に一対一に対応するように解読鍵402(D-Key#0~D-Key#255)が256種類登録されている。解読鍵読み出し回路218は暗号化鍵で一意に定まる解読鍵を読み出し、解読回路221に転送する。解読回路221は、バッファ220より入力するパケットを解読鍵を用いて解読し、LAN制御部180に転送する。

【0061】次に本実施例におけるカウント値／暗号化鍵／解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(FD)より設定データをロードする。カウント値／暗号化鍵を登録するメモリ213への設定データの書き込み制御はメモリ#1書込制御222が行う。一方、暗号化鍵／解読鍵を登録するメモリ219への設定データの書き込み制御はメモリ219の書込制御223が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ213の書込制御222およびメモリ219の書込制御223に転送される。書込制御222および223はCPU120の指示に基づき、メモリ213およびメモリ219の登録内容の書き換えを行う。



【0062】次に図15、図16および図17を用いて第六の実施例について説明する。第一の実施例が暗号化鍵IDを暗号化情報と共に転送するのに対して、本実施例は解読鍵を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部200の動作のみが異なるので、暗号化部200のみ説明する。

【0063】図15において、入力パケットカウント回路211はLAN制御部180から入力するパケット数をカウントし、カウント値を暗号化鍵/解読鍵読み出し回路234に転送する。暗号化鍵/解読鍵読み出し回路234はカウント値に基づき、パケットの暗号化に使用する暗号化鍵および解読時に使用する解読鍵をメモリ213より読み出す。

【0064】図16にメモリ213の構成例を示す。本実施例では0から255までのカウント値301に対して、一対一に対応するように暗号化鍵302と解読鍵307が256組登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵/解読鍵を対応させることも可能である。そのような場合には256種類のカウント値に対して256組以下の暗号化鍵/解読鍵が登録される。更に、暗号化鍵/解読鍵読み出し回路234は暗号化鍵を暗号化回路215に転送すると共に、解読鍵を解読鍵挿入回路235に転送する。バッファ214は暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。解読鍵挿入回路232はパケットの所定の位置に、暗号化鍵/解読鍵読み出し回路234より転送された解読鍵を挿入する。

【0065】図17に本実施例における解読鍵507の挿入位置を示す。パケット500はパケットヘッダと情報領域501から構成される。パケットヘッダ内には宛先アドレス502と送信元アドレス503が書き込まれている。解読鍵507はユーザ情報505とパケットヘッダの間に挿入する。MAC層では、解読鍵507とユーザ情報505を情報領域501として取扱うので、解読鍵507の挿入はMAC層プロトコルには影響を及ぼさない。

【0066】暗号化回路215はバッファ214より入力するパケットを暗号化し、解読鍵挿入回路235に転送する。本実施例では、解読鍵は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ213より読み出した個別の暗号化鍵を用いて暗号化する。

【0067】次に、LANから暗号化情報を受信したときの処理について説明する。解読鍵分離回路236は受信暗号化パケットから解読鍵の区間を切り出し、解読回路221に転送する。解読鍵は共通暗号化鍵で暗号化されているので、全ての受信端末は解読鍵を解読することができる。また、解読鍵を暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には解読鍵分離回路236が切り出した解読鍵をそのまま用いる。解読回路221は解読鍵分離回路236より転送さ

れるパケットを当該解読鍵を用いて解読し、LAN制御部180に転送する。

【0068】次に本実施例におけるカウント値/暗号化鍵/解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(FD)より設定データをロードする。カウント値/暗号化鍵/解読鍵を登録するメモリ213への設定データの書き込み制御はメモリ213の書き込み制御222が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ213の書き込み制御222に転送される。書き込み制御222はCPU120の指示に基づきメモリ213の登録内容の書き換えを行う。

【0069】次に図18、図19および20を用いて第七の実施例について説明する。第一の実施例が暗号化鍵IDを暗号化情報と共に転送するのに対して、本実施例は解読鍵識別子(以下、解読鍵IDと称す)を暗号化情報と共に転送する。尚、本実施例も第一の実施例と暗号化部200の動作のみが異なるので、暗号化部200のみ説明する。

【0070】図18において、入力パケットカウント回路211はLAN制御部180から入力するパケット数をカウントし、カウント値を暗号化鍵/ID読み出し回路212に転送する。暗号化鍵/ID読み出し回路212はカウント値に基づき、パケットの暗号化に使用する暗号化鍵と暗号化鍵に対応する解読鍵を一意に示す解読鍵IDをメモリ213より読み出す。

【0071】図19(a)にメモリ213の構成例を示す。本実施例では0から255までのカウント値301に対して、一対一に対応するように暗号化鍵302と解読鍵ID308が256組登録されている。尚、異なる複数のカウント値に対して同一の暗号化鍵/解読鍵IDを対応させることも可能である。そのような場合には256種類のカウント値に対して256組以下の暗号化鍵/解読鍵IDが登録される。更に、暗号化鍵/解読鍵読み出し回路212は暗号化鍵を暗号化回路215に転送すると共に、解読鍵IDを解読鍵ID挿入回路237に転送する。バッファ214は暗号化鍵の転送までの時間だけLAN制御部180から入力したパケットを格納する。解読鍵ID挿入回路237はパケットの所定の位置に、暗号化鍵/ID読み出し回路212より転送された解読鍵IDを挿入する。

【0072】図20に本実施例における解読鍵ID508の挿入位置を示す。パケット500はパケットヘッダと情報領域501から構成される。パケットヘッダ内には宛先アドレス502と送信元アドレス503が書き込まれている。解読鍵ID508はユーザ情報505とパケットヘッダの間に挿入する。MAC層では、解読鍵ID



19

508とユーザ情報505を情報領域501として取扱うので、解読鍵ID508の挿入はMAC層プロトコルには影響を及ぼさない。

【0073】暗号化回路215はバッファ214より入力するパケットを暗号化し、解読鍵ID挿入回路237に転送する。本実施例では、解読鍵は共通暗号化鍵を用いて暗号化し、その他の部分はメモリ213より読み出した個別の暗号化鍵を用いて暗号化する。

【0074】次に、LANから暗号化情報を受信したときの処理について説明する。解読鍵ID分離回路237は受信暗号化パケットから解読鍵IDの区間を切り出し、解読鍵読み出し回路218に転送する。解読鍵ID以外の部分はそのままバッファ220に格納される。解読鍵読み出し回路218は前記解読鍵IDに基づき、メモリ219より解読鍵を読み出す。解読鍵IDは共通暗号化鍵で暗号化されているので、全ての受信端末は解読鍵IDを解読することができる。尚、本実施例では解読鍵IDの暗号化に共通暗号化鍵を用いていることから平文の解読鍵IDと暗号化した解読鍵IDは一対一に対応するので、受信したパケットの解読鍵IDを解読せずに用いて解読鍵を選択することも可能である。また、解読鍵IDを暗号化せずにその他の暗号化情報と共に転送することも可能であり、その場合には解読鍵ID分離回路238が切り出した解読鍵IDをそのまま用いて解読鍵の選択を行う。

【0075】図19(b)にメモリ219の構成例を示す。本実施例では256種類の解読鍵ID407に一対一に対応するように解読鍵402が256種類登録されている。解読鍵読み出し回路218は解読鍵IDで一意に定まる解読鍵を読み出し、解読回路221に転送する。解読回路221は、バッファ220より入力するパケットを解読鍵を用いて解読し、LAN制御部180に転送する。

【0076】次に本実施例におけるカウント値/暗号化鍵/解読鍵ID/解読鍵の設定方法について説明する。本実施例ではシステム構築時に、フロッピーディスク(FD)より設定データをロードする。カウント値/暗号化鍵/解読鍵IDを登録するメモリ213への設定データの書き込み制御はメモリ213の書込制御222が行う。解読鍵ID/解読鍵を登録するメモリ219への設定データの書き込み制御はメモリ219の書込制御223が行う。尚、設定データの変更が生じた場合には、ネットワーク内の通信端末あるいは制御端末からのコマンド入力によりメモリ内の登録内容の書き換えを行う。この場合には、WS本体100内のCPU120で処理された設定データが内部バス160を介してメモリ213の書込制御222に転送される。書込制御222はCPU120の指示に基づきメモリ213およびメモリ219の登録内容の書き換えを行う。

【0077】次に図21、図22を用いて第八の実施例

20

について説明する。第七の実施例は第一の実施例とメモリ213、メモリ219の設定方法が異なる。即ち、第一の実施例ではメモリ213、219の設定はFDより設定データをローディングすることにより行った。本実施例では、図21に示すようにメモリ213、219の設定データはLANインタフェース140内のROM191から読み込む。

【0078】図22において、書込制御239はROM191よりメモリ213への設定データ(カウント値/暗号化鍵/暗号化鍵ID)を読み込み、メモリ213に書き込む。書込制御240はROM191よりメモリ219への設定データ(暗号化鍵ID/解読鍵)を読み込み、メモリ219に書き込む。

【0079】尚、本実施例を前記第二ないし第七の実施例に適用することは容易である。第二の実施例に適用する場合には、ROM191に記憶する内容を、メモリ213用として送信パケット宛先アドレス/暗号化鍵とし、メモリ219用として受信パケット宛先アドレス/解読鍵とすれば良い。第三の実施例に適用する場合には、ROM191に記憶する内容を、メモリ213用として送信パケットルート情報/暗号化鍵とし、メモリ219用として受信パケットルート情報/解読鍵とすれば良い。第四の実施例に適用する場合には、ROM191に記憶する内容を、メモリ213用として送信パケット送信元アドレス/暗号化鍵、メモリ219用として受信パケット送信元アドレス/解読鍵とすれば良い。第五の実施例に適用する場合には、ROM191に記憶する内容を、メモリ213用としてカウント値/暗号化鍵、メモリ219用として暗号化鍵/解読鍵とすれば良い。第六の実施例に適用する場合には、ROM191に記憶する内容を、メモリ213用としてカウント値/暗号化鍵/解読鍵とすれば良い。第七の実施例に適用する場合には、ROM191に記憶する内容を、メモリ213用としてカウント値/暗号化鍵/解読鍵ID、メモリ219用として解読鍵ID/解読鍵とすれば良い。

【0080】

【発明の効果】本発明によれば、暗号化情報と共に暗号化鍵/解読鍵を一意に示す識別情報を転送するので、複数の暗号化鍵を用いる秘匿通信においても暗号化情報を正確に解読することができる。

【0081】識別情報として暗号化鍵あるいは解読鍵そのものを用いる場合には、任意の通信端末に対して任意の暗号化鍵を用いることが出来るので、秘匿通信の信頼性がより向上する。

【0082】識別情報として暗号化鍵識別子あるいは解読鍵識別子を用いる場合には、任意の通信端末に対して任意の暗号化鍵を用いることが出来ることに加えて、暗号化鍵あるいは解読鍵を識別子として表現しているので、更に秘匿通信の信頼性が向上する。

【0083】識別情報として端末アドレスあるいはルー

ト情報を用いる場合には、特別な識別子を使用することなく暗号化鍵／解読鍵を特定することが出来る。

【図面の簡単な説明】

【図1】本発明の第一の実施例における暗号化部のブロック図。

【図2】本発明の第一の実施例における通信端末（WS）本体のブロック図。

【図3】本発明の第一の実施例におけるLANインタフェースのブロック図。

【図4】本発明の第一の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図5】本発明の第一の実施例におけるパケットの説明図。

【図6】本発明の第二の実施例における暗号化部のブロック図。

【図7】本発明の第二の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図8】本発明の第三の実施例における暗号化部のブロック図。

【図9】本発明の第三の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図10】本発明の第四の実施例における暗号化部のブロック図。

【図11】本発明の第四の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図12】本発明の第五の実施例における暗号化部のブロック図。

【図13】本発明の第五の実施例における暗号化鍵記憶部および解読鍵記憶部の説明図。

【図14】本発明の第五の実施例におけるパケットの説明図。

【図15】本発明の第六の実施例における暗号化部のブロック図。

【図16】本発明の第六の実施例における暗号化鍵および解読鍵記憶部の説明図。

【図17】本発明の第六の実施例におけるパケットの説明図。

【図18】本発明の第七の実施例における暗号化部のブロック図。

【図19】本発明の第七の実施例における暗号化鍵記憶部および解読鍵記憶部の構成図。

【図20】本発明の第七の実施例におけるパケットの説明図。

【図21】本発明の第八の実施例におけるLANインタフェースのブロック図。

【図22】本発明の第八の実施例における暗号化部のブロック図。

【符号の説明】

200…暗号化部、211…入力パケットカウント回路、212…暗号化鍵／ID読み出し回路、213…メモリ、215…暗号化回路、216…暗号化鍵ID挿入回路、217…暗号化鍵ID分離回路、218…解読鍵読み出し回路、219…メモリ、221…解読回路、222…メモリ書込制御、223…メモリ書込制御。

【図9】

【図11】

【図16】

図9

(A)

送信パケット ルート情報	暗号化鍵
VCN#0	C-Key#0
VCN#1	C-Key#1
⋮	⋮
VCN#254	C-Key#254
VCN#255	C-Key#255

(B)

受信パケット ルート情報	解読鍵
VCN#0	D-Key#0
VCN#1	D-Key#1
⋮	⋮
VCN#254	D-Key#254
VCN#255	D-Key#255

図11

(A)

送信パケット 送信元アドレス	暗号化鍵
SA#0	C-Key#0

(B)

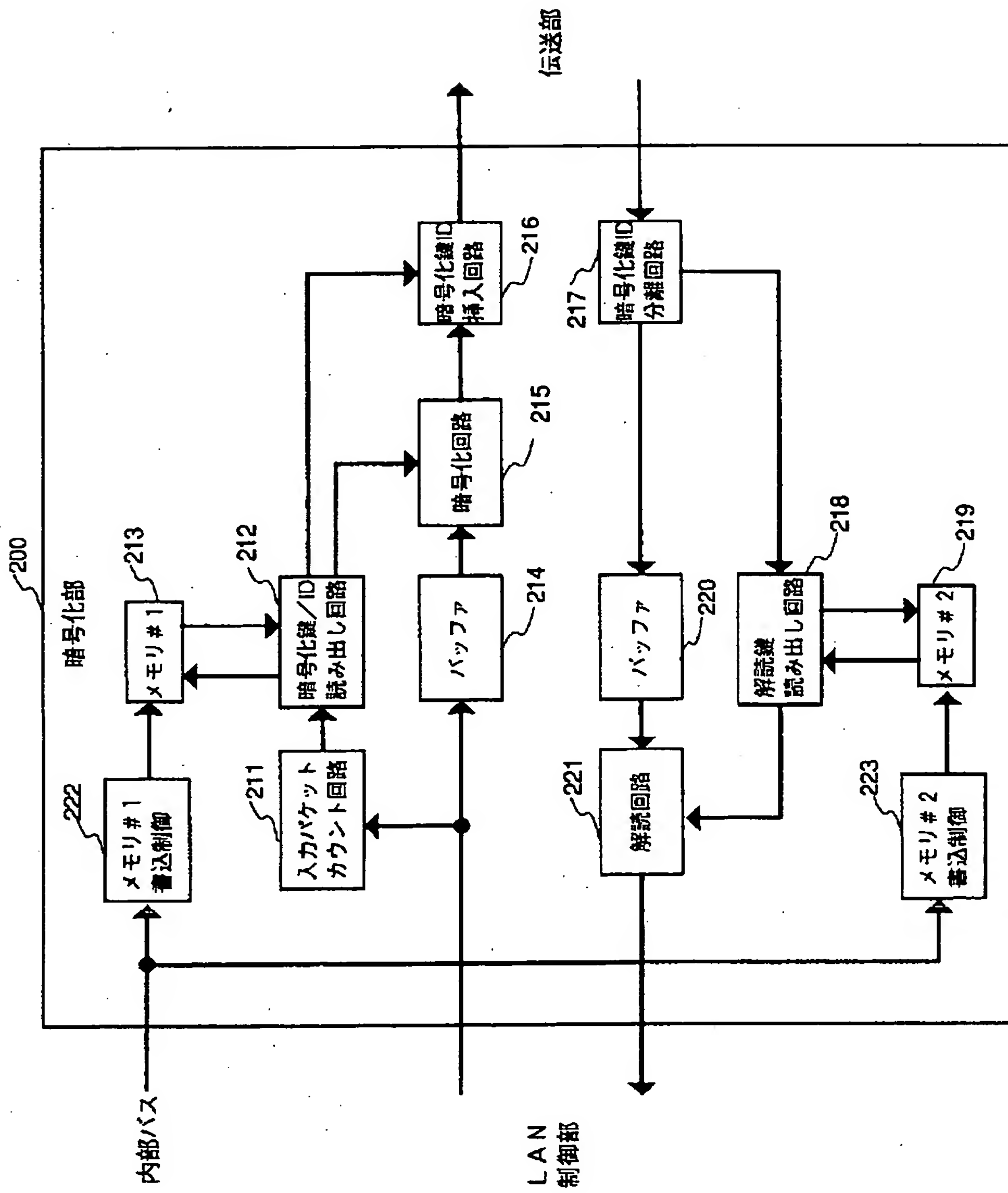
受信パケット 送信元アドレス	解読鍵
SA#0	D-Key#0
SA#1	D-Key#1
⋮	⋮
SA#254	D-Key#254
SA#255	D-Key#255

図16

カウント値	暗号化鍵	解読鍵
0	C-Key#0	D-Key#0
1	C-Key#1	D-Key#1
⋮	⋮	⋮
254	C-Key#254	D-Key#254
255	C-Key#255	D-Key#255

【図1】

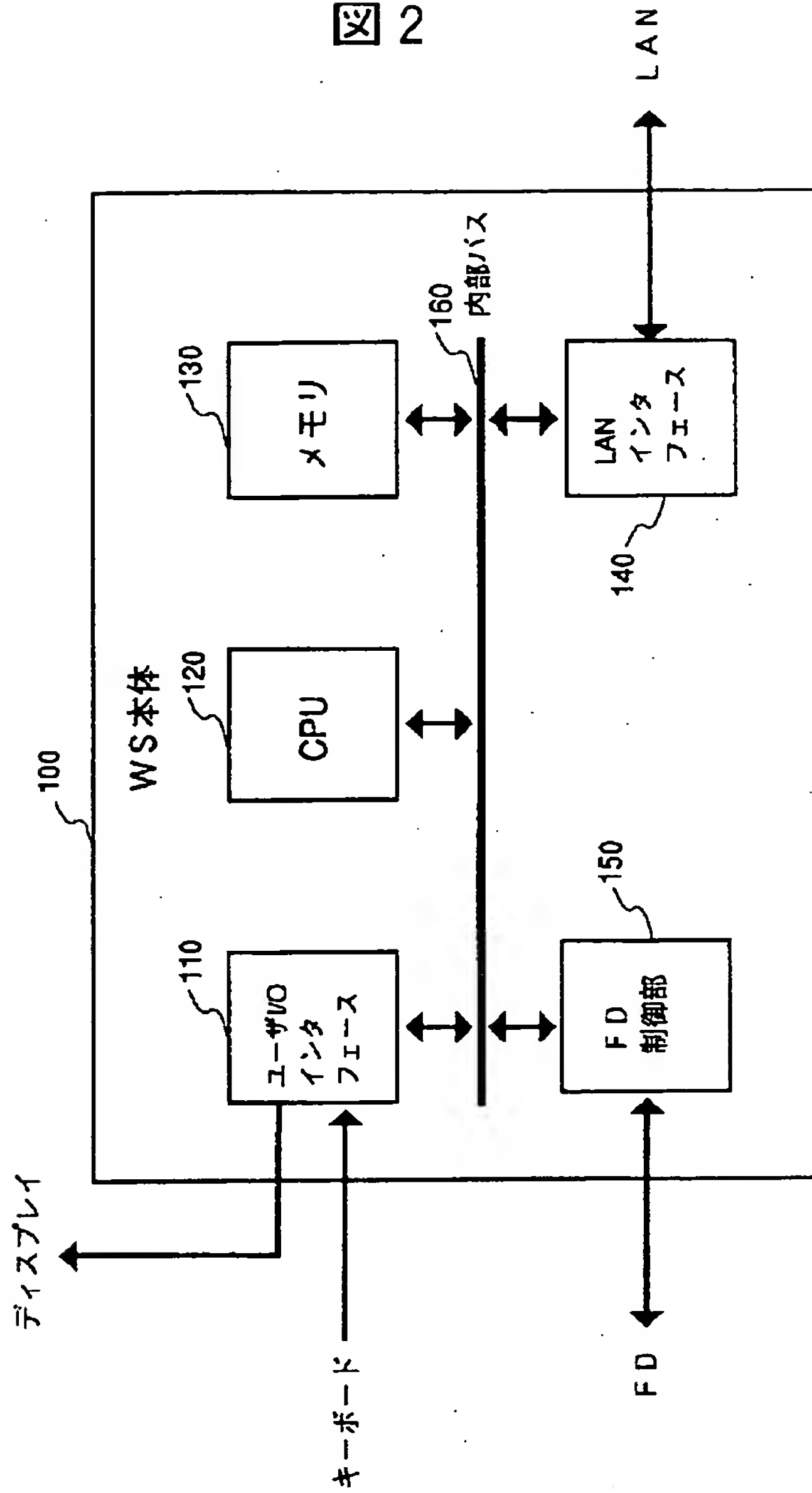
図 1





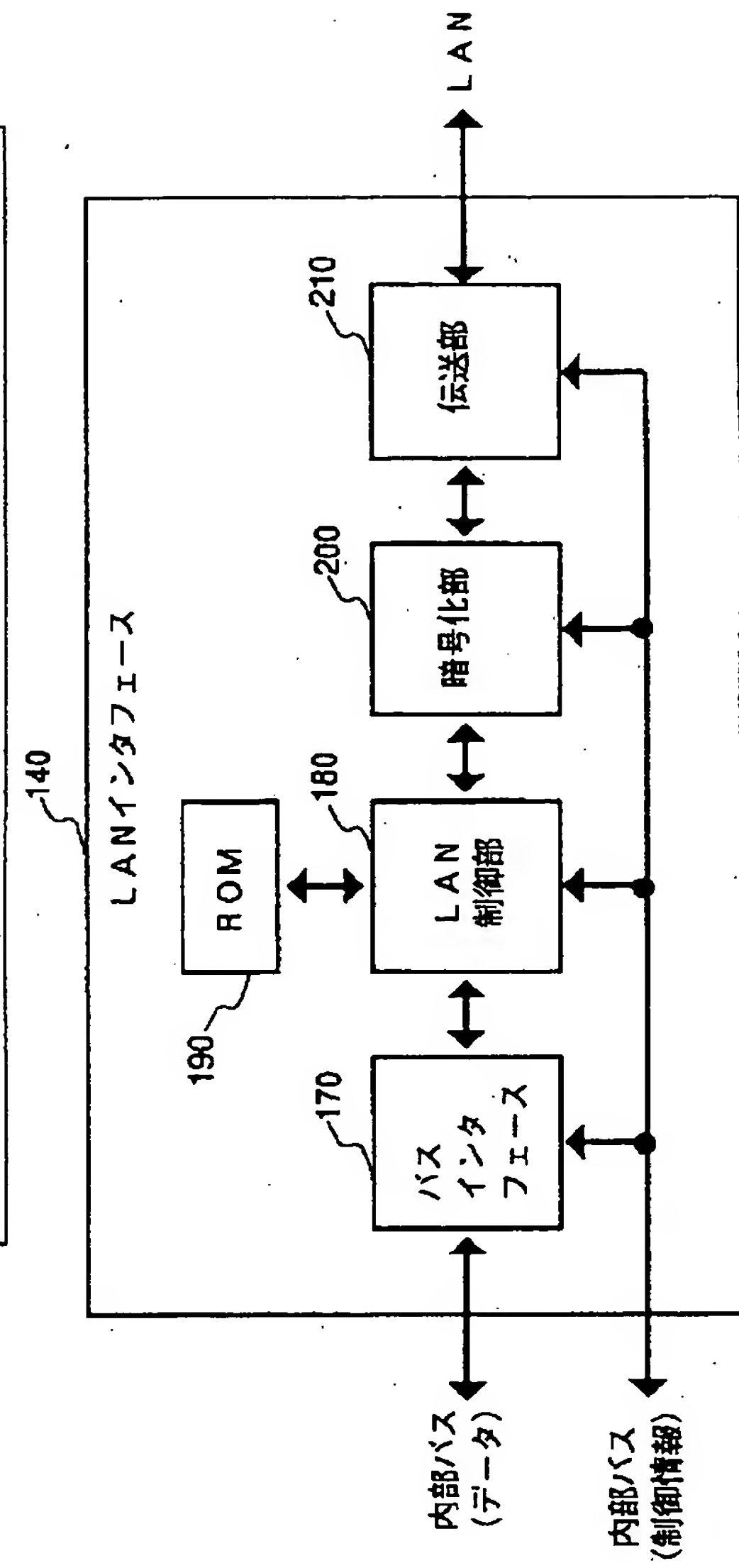
【図2】

図 2



【図3】

図 3



【図4】

図4

(a)

301 カウント値	302 暗号化鍵	303 暗号化ID (H)
0	C-Key#0	00
1	C-Key#1	01
⋮	⋮	⋮
254	C-Key#254	FE
255	C-Key#255	FF

【図7】

図7

(a)

304 送信パケット宛先アドレス	303 暗号化鍵
DA#0	C-Key#0
DA#1	C-Key#1
⋮	⋮
DA#254	C-Key#254
DA#255	C-Key#255

(b)

401 暗号化ID (H)	402 解暗鍵
00	D-Key#0
01	D-Key#1
⋮	⋮
FE	D-Key#254
FF	D-Key#255

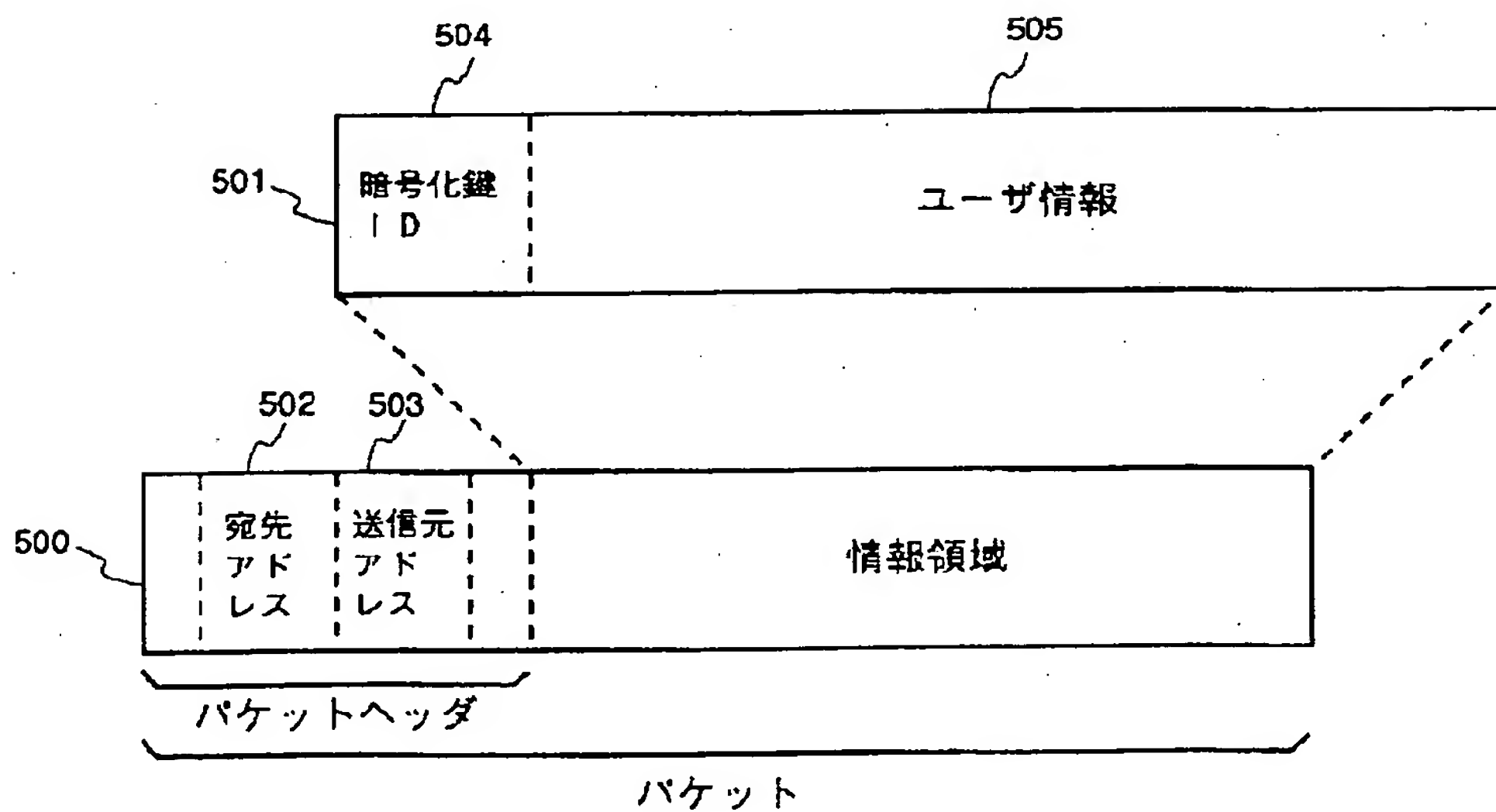
(b)

403 受信パケット宛先アドレス	402 解暗鍵
自アドレス	D-Key#X <sub>1</sub>
グループアドレス#1	D-Key#X <sub>2</sub>
⋮	⋮
グループアドレス#N	D-Key#X <sub>N+1</sub>
一斉同報アドレス	D-Key#X <sub>N+2</sub>

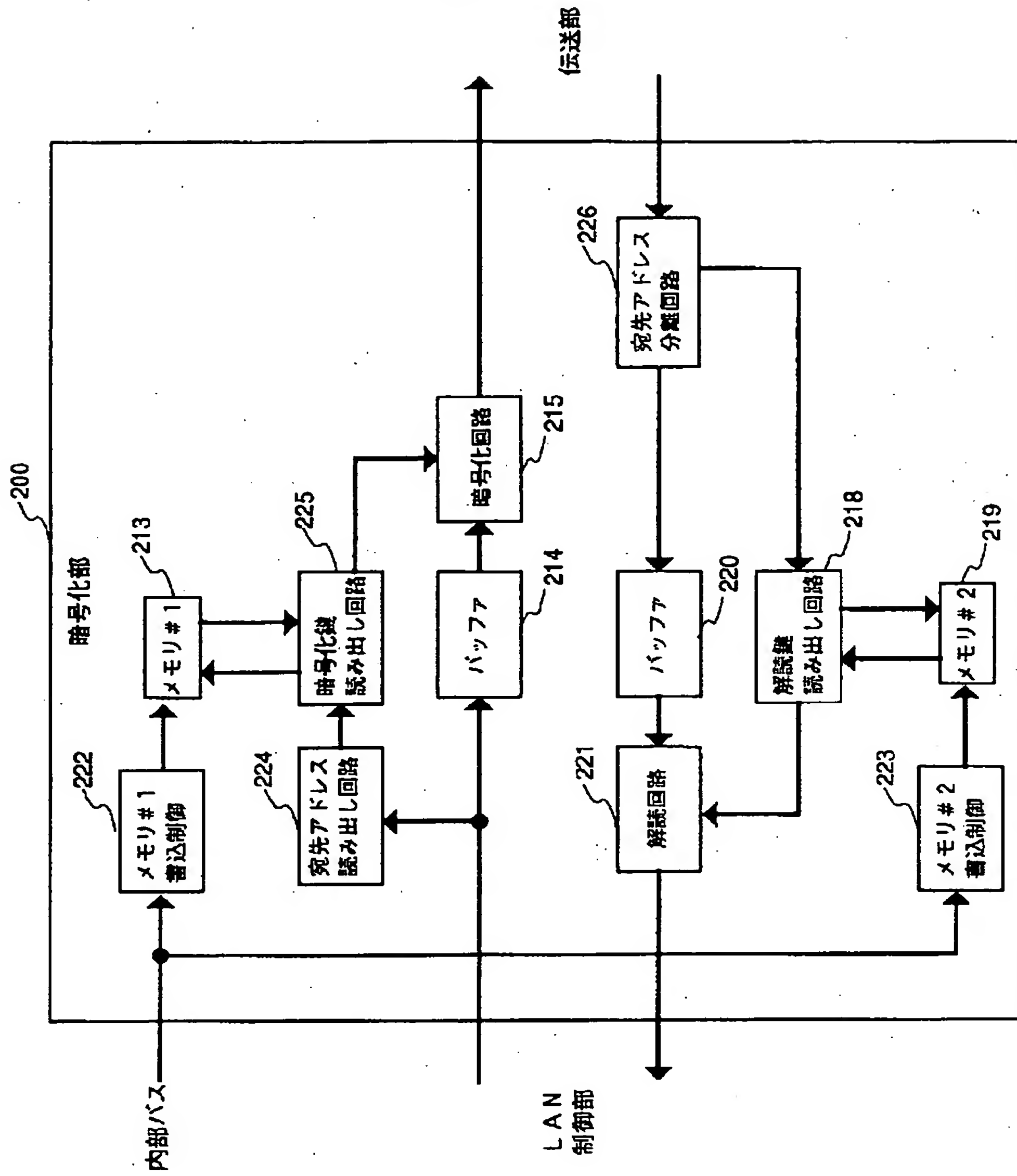
但し、 $0 \leq X_i \leq 255$  ( $1 \leq i \leq N+2$ )

【図5】

図5



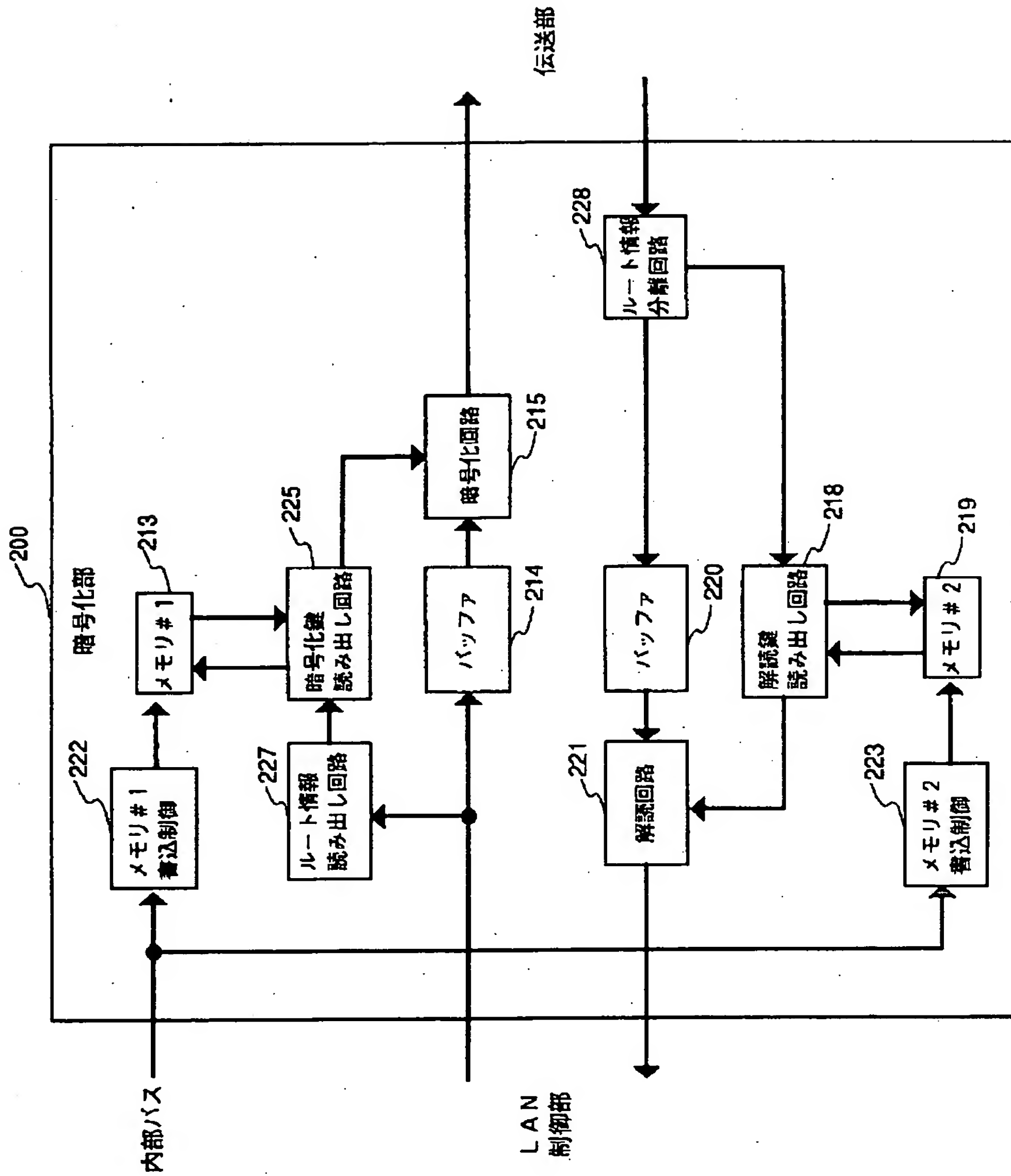
【図6】





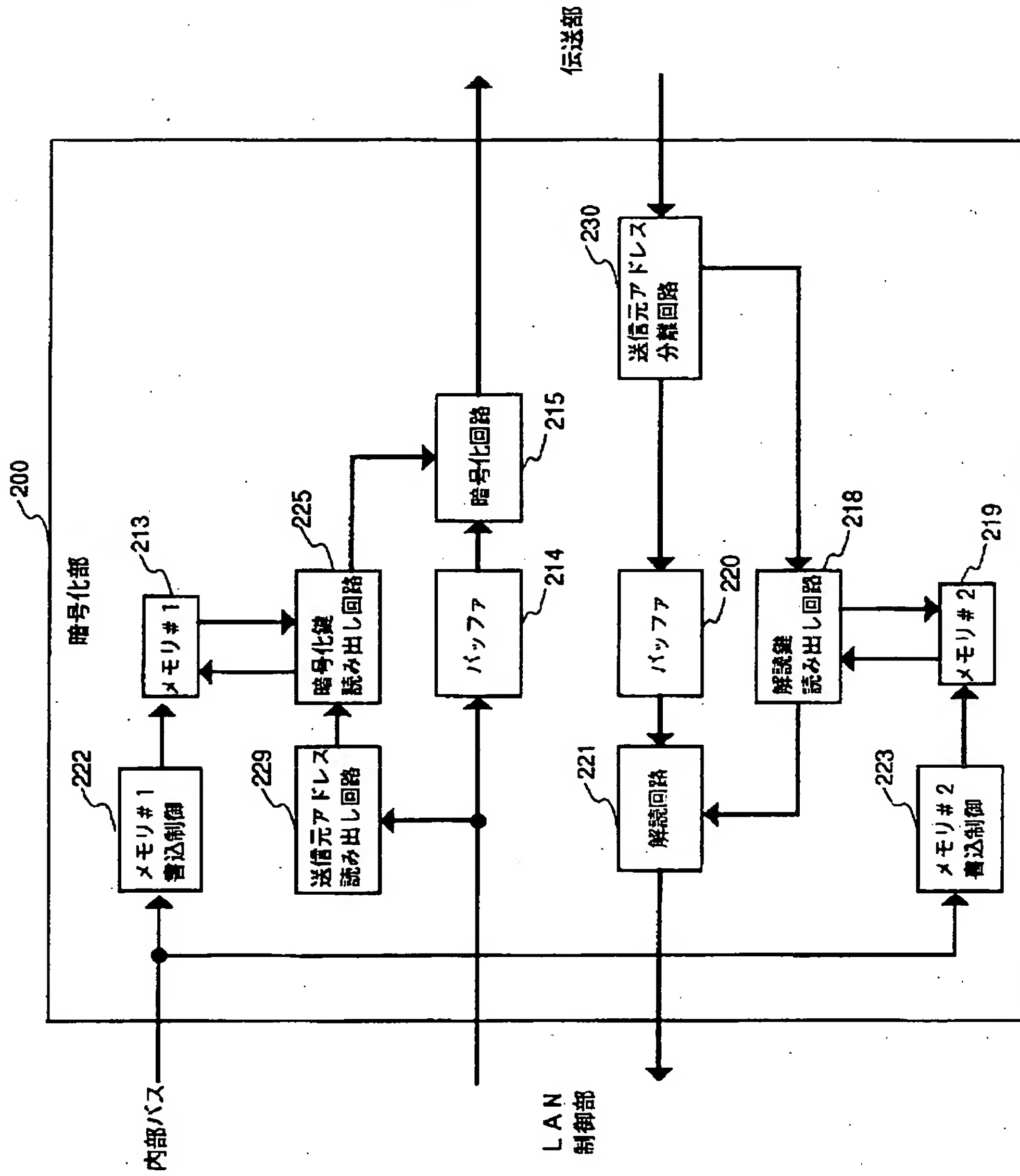
【図8】

図8



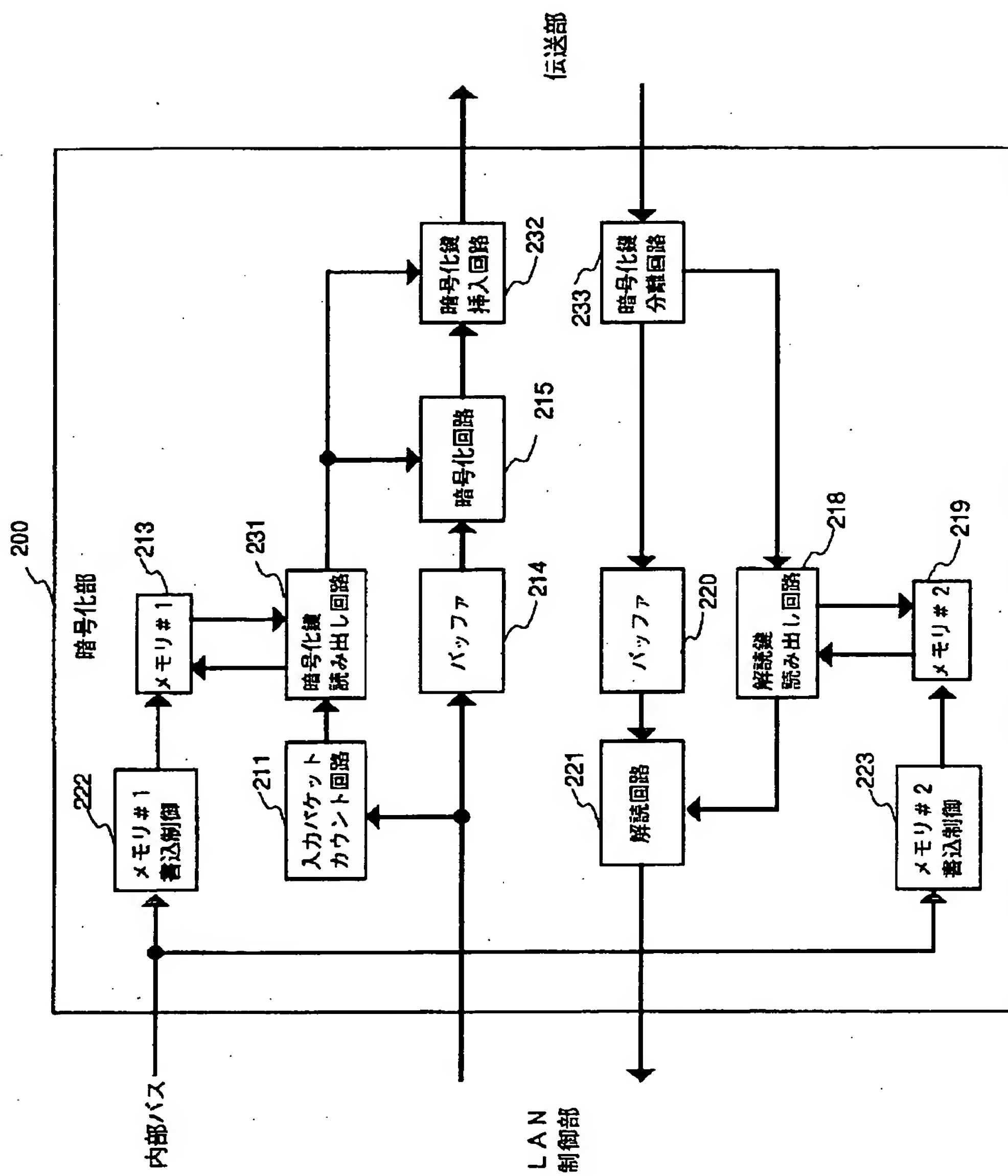
【図10】

図 10



【図12】

図12





【図13】

図13

(a)

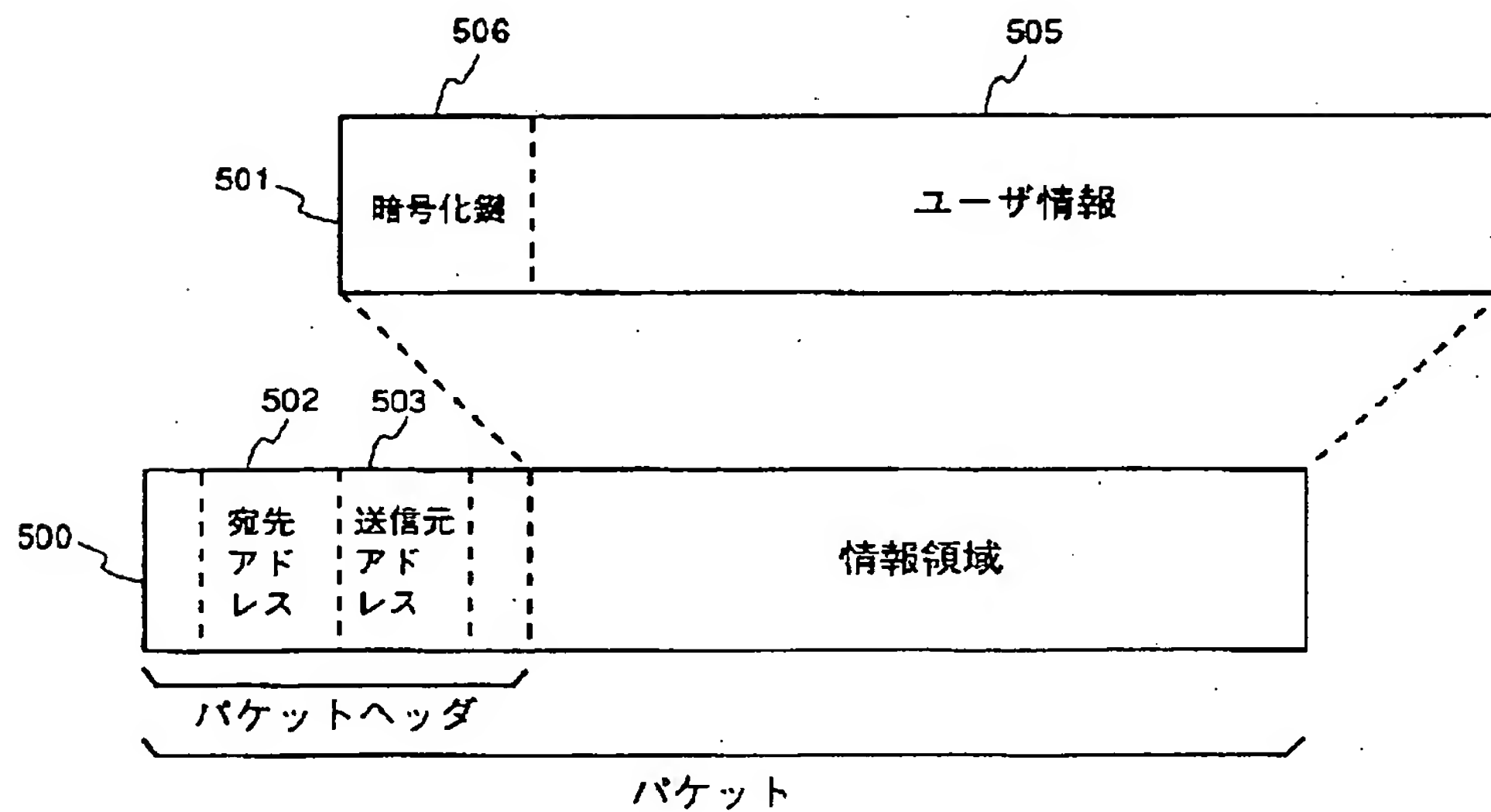
301 カウント値	302 暗号化鍵
0	C-Key#0
1	C-Key#1
⋮	⋮
254	C-Key#254
255	C-Key#255

(b)

406 暗号化鍵	402 解読鍵
C-Key#0	D-Key#0
C-Key#1	D-Key#1
⋮	⋮
C-Key#254	D-Key#254
C-Key#255	D-Key#255

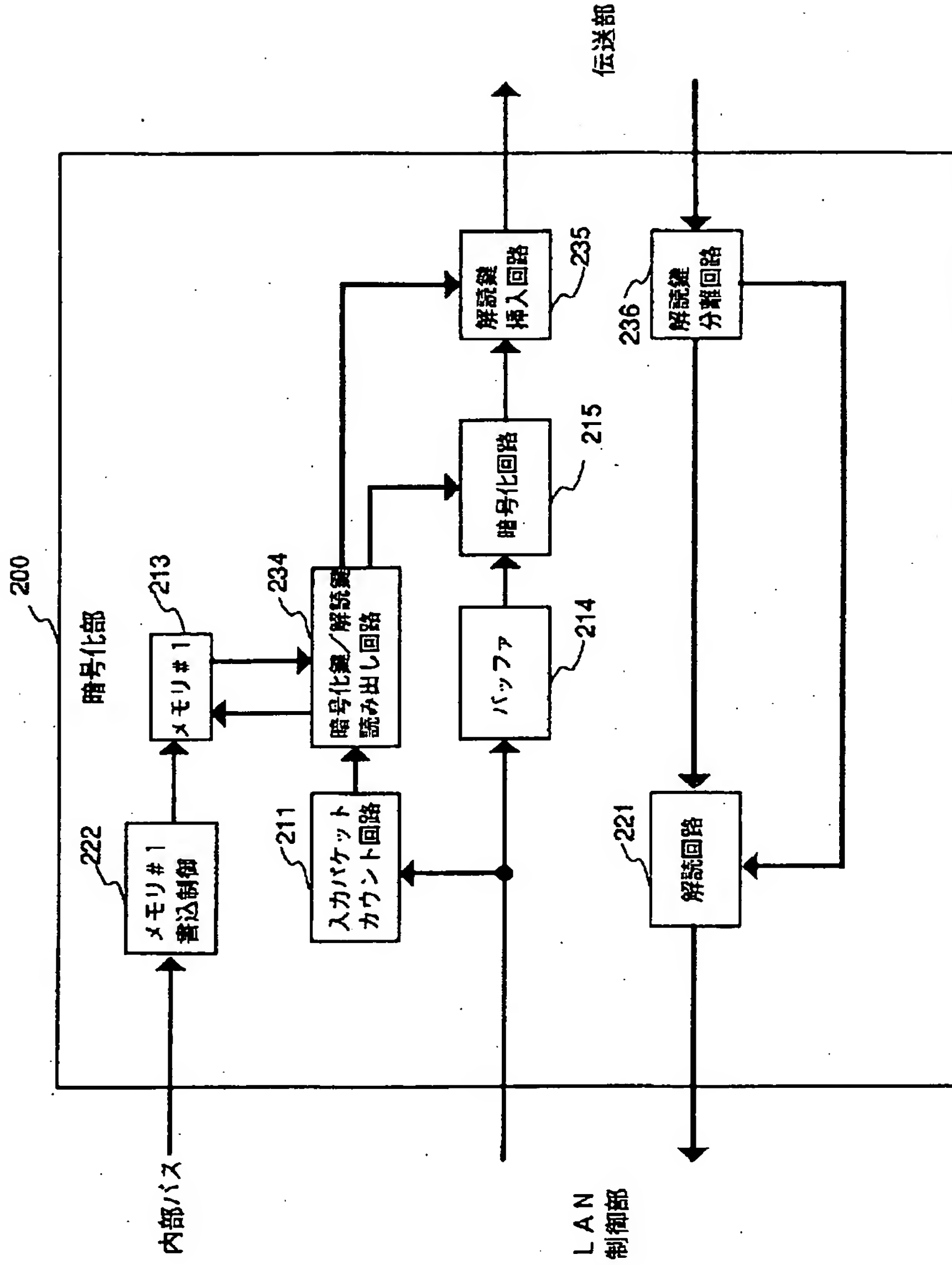
【図14】

図14



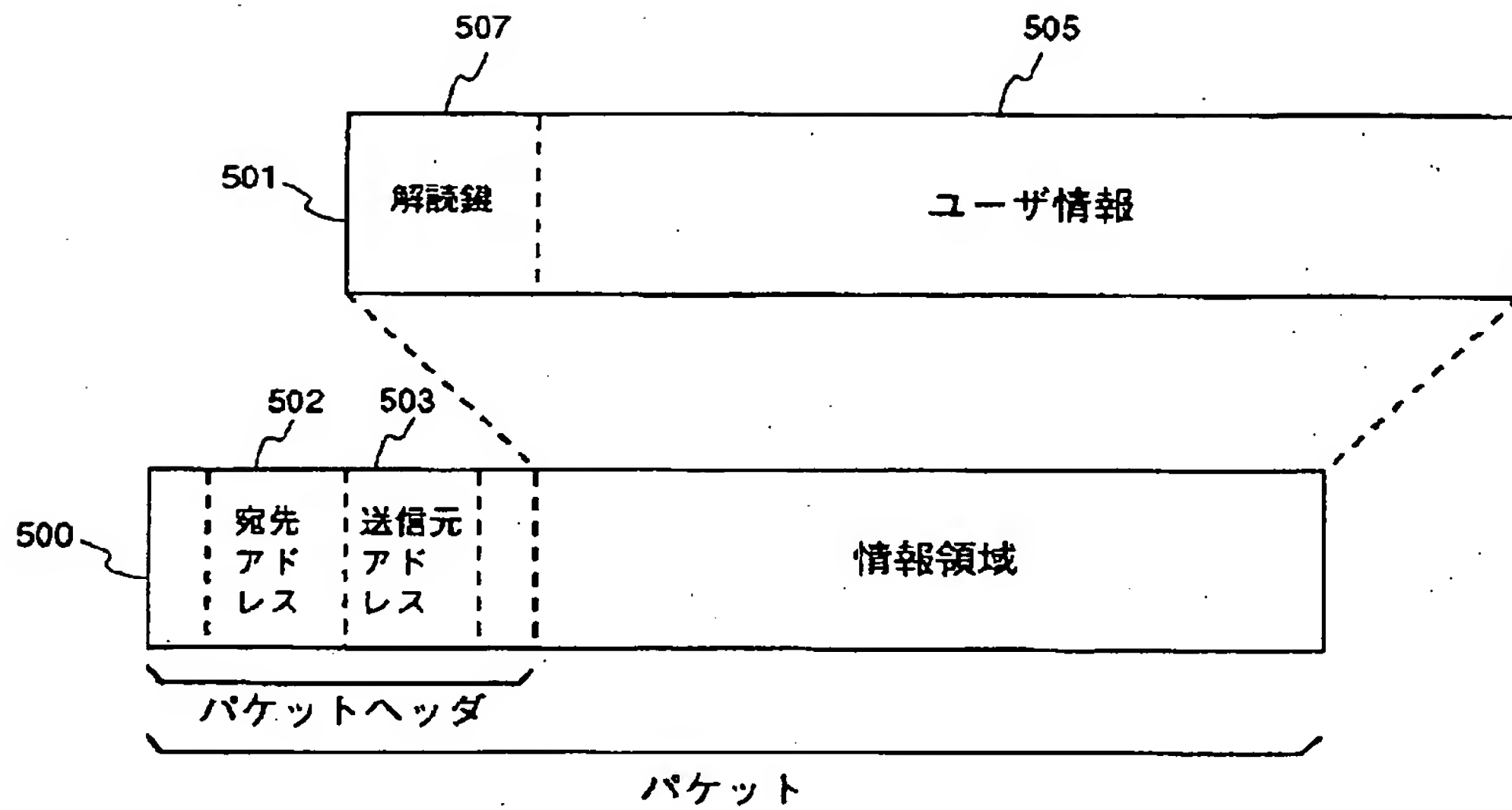
【図15】

図15



【図17】

図17



【図19】

図19

(a)

301 カウンタ値	302 暗号化値	303 解読鍵ID (H)
0	C-Key#0	00
1	C-Key#1	01
⋮	⋮	⋮
254	C-Key#254	FE
255	C-Key#255	FF

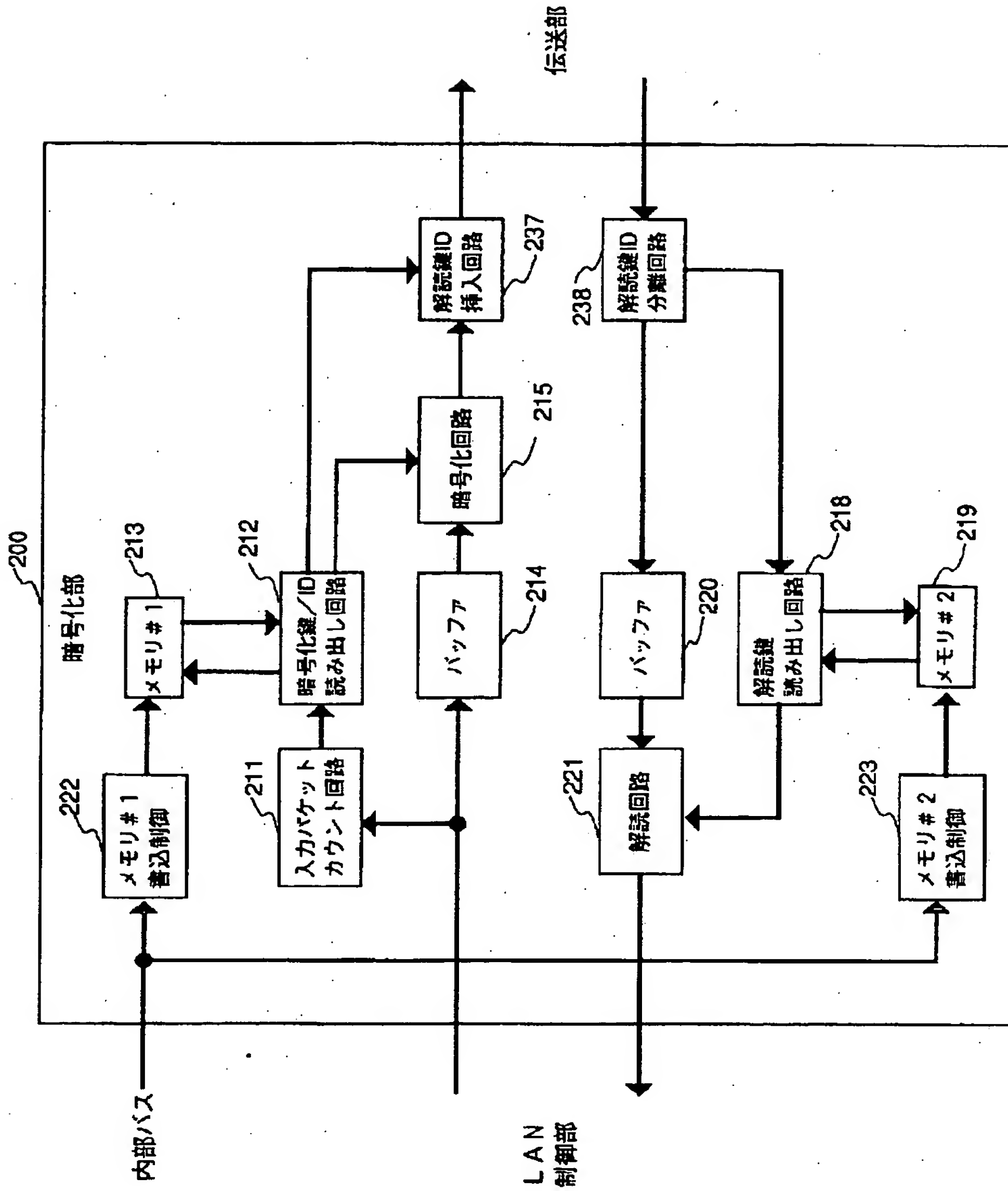
(b)

407 解読鍵ID (H)	402 解読鍵
00	D-Key#0
01	D-Key#1
⋮	⋮
FE	D-Key#254
FF	D-Key#255



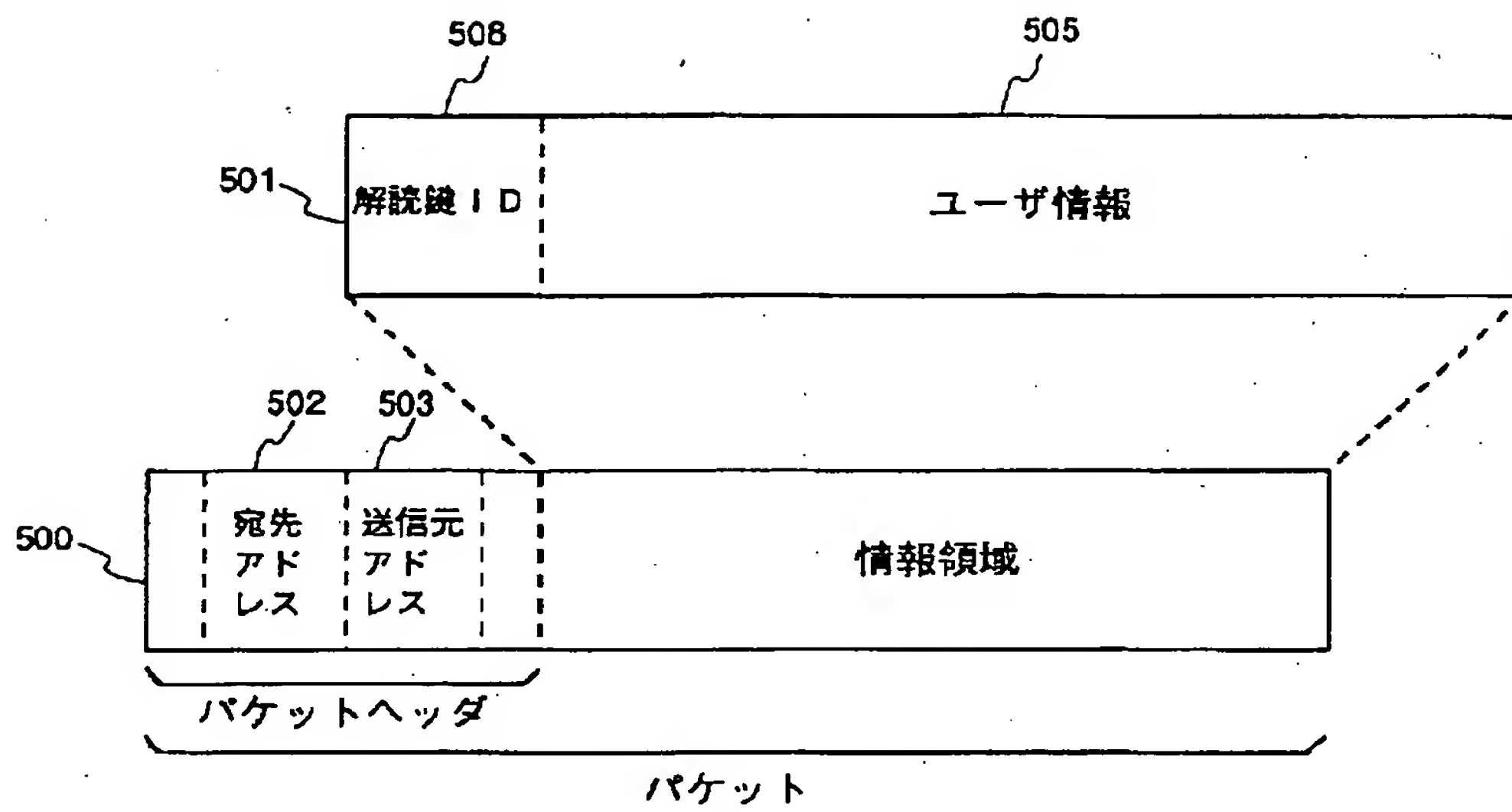
【図18】

図18



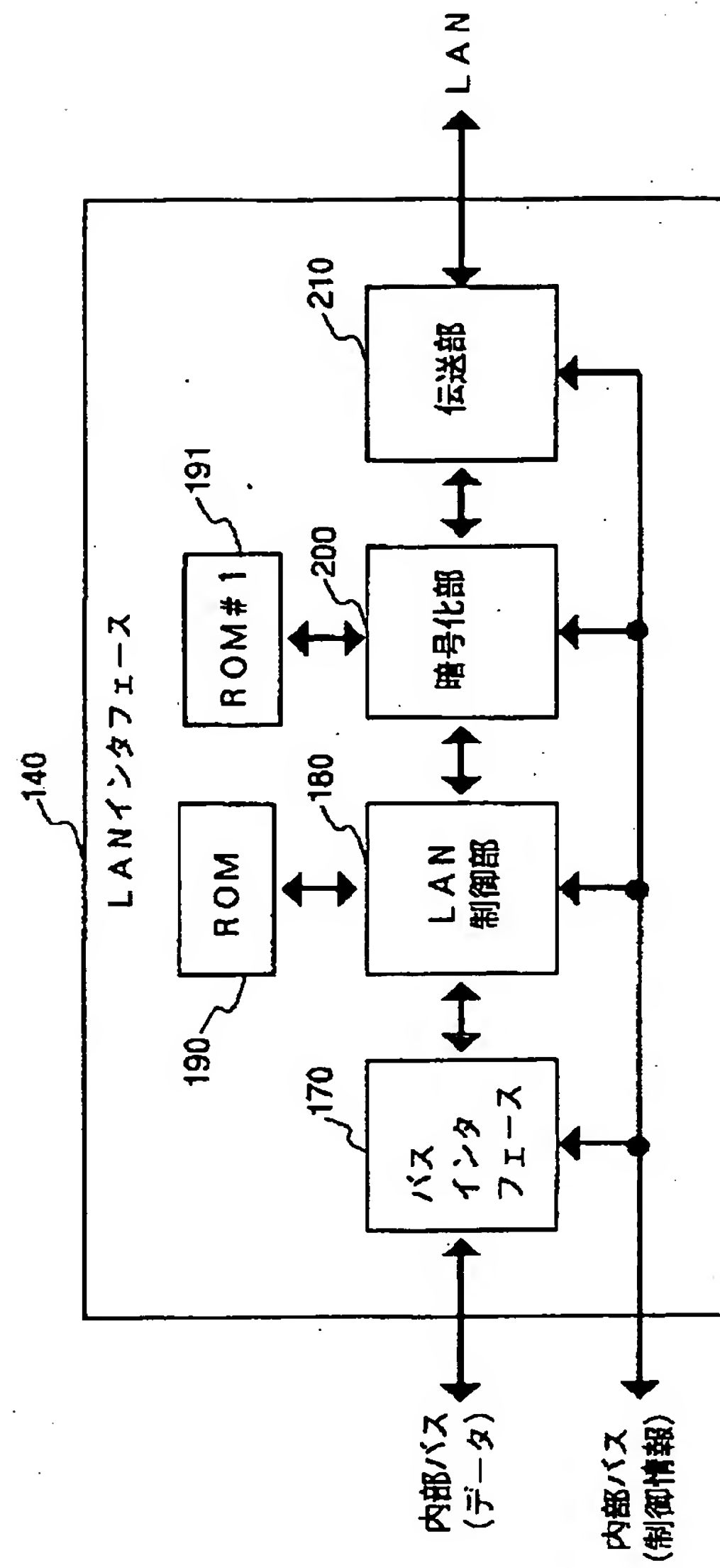
【図20】

図20



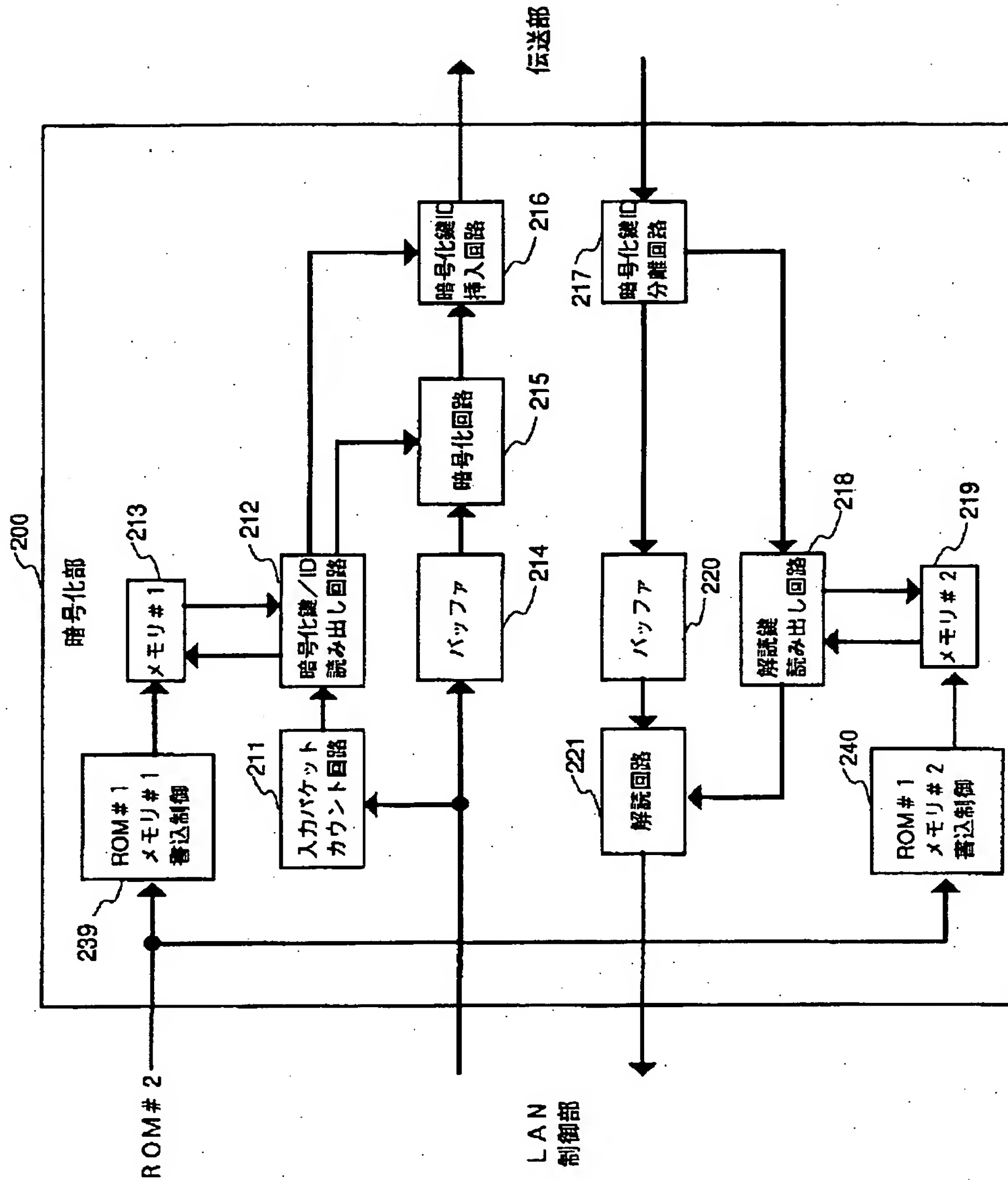
【図21】

図 2 1



【図22】

図 2 2



フロントページの続き

(51) Int. Cl. 5

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 12/28



(72)発明者 鈴木 秀哉  
東京都国分寺市東恋ヶ窪1丁目280番地  
株式会社日立製作所中央研究所内